

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
29 March 2001 (29.03.2001)

PCT

(10) International Publication Number
WO 01/22200 A2

(51) International Patent Classification⁷:

G06F

(74) Agents: DALEY-WATSON, Christopher, J. et al.;
Perkins Coie LLP, Suite 4800, 1201 Third Avenue, Seattle,
WA 98101-3099 (US).

(21) International Application Number: PCT/US00/07986

(22) International Filing Date: 24 March 2000 (24.03.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/126,080 25 March 1999 (25.03.1999) US
60/149,621 16 August 1999 (16.08.1999) US

(71) Applicant (for all designated States except US): VOTE-HERE, INC. [US/US]; Suite 250, 3101 Northup Way, Bellevue, WA 98004 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): GREEN, Richard, L. [US/US]; 190 Lyme Road, Hanover, NH 03755 (US). ADLER, Jim [US/US]; Suite 250, 3101 Northup Way, Bellevue, WA 98004 (US).

(81) Designated States (national): AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW.

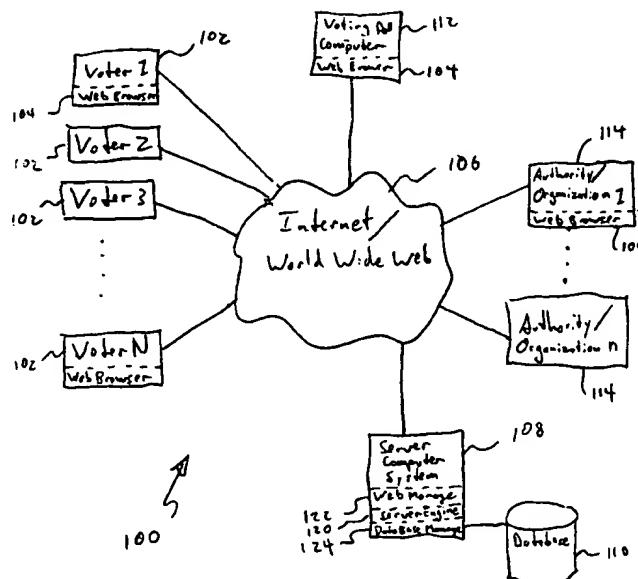
(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TI, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

— Without international search report and to be republished upon receipt of that report.

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: ELECTRONIC VOTING SCHEME EMPLOYING PERMANENT BALLOT STORAGE



WO 01/22200 A2

(57) Abstract: Disclosed is a system for recording records, such as electronic ballots in an electronic scheme. A web server posts a web page having a ballot box. Individual voters receive and submit to the web page electronic ballots reflecting their votes. The web server computer permanently stores each received electronic ballots using a Write-Once, Read-Many (WORM) drive or similar device to prevent ballots from later being erased or altered. Election results may then be tallied, and the results of such tallying, together with the received ballots, transmitted or provided to a third-party authority to review the election results.

ELECTRONIC VOTING SCHEME EMPLOYING PERMANENT BALLOT STORAGE

CROSS-REFERENCE TO RELATED APPLICATION

This application claims the benefit of U.S. Provisional Patent
5 Applications, having numbers 60/126,080 and 60/149,621, filed March 25, 1999,
and August 16, 1999, respectively, both of which are currently pending.

TECHNICAL FIELD

The following relates generally to electronic voting schemes.

BACKGROUND

10 The Internet is increasingly being used to conduct a variety of activities, including research, communication or document exchange, and "electronic commerce," in part, because it facilitates electronic communications with large databases, between individuals, and between vendors and purchasers. The Internet comprises a vast number of computers and computer networks
15 interconnected through communication channels. One individual can use a personal computer to connect via the Internet to another's computer. In the field of electronic commerce, although many commercial transactions performed today could be performed electronically, the acceptance and wide-spread use of electronic commerce depends, in large part, upon the ease-of-use of conducting
20 such electronic commerce or other activities. For example, if electronic commerce can be easily conducted, then even the novice computer user will choose to engage in such activities. Therefore, it is important that techniques be developed to facilitate conducting such activities electronically.

The Internet facilitates conducting activities electronically, in part,
25 because it uses standardized techniques for exchanging information. Many standards have been established for exchanging information over the Internet,

such as electronic mail, Gopher, and the World Wide Web (“WWW”). The WWW service allows a server computer system (*i.e.*, web server or web site) to send graphical web pages of information to a remote client computer system. The remote client computer system can then display the web pages. Each resource 5 (e.g., computer or web page) of the WWW is uniquely identifiable by a Uniform Resource Locator (“URL”). To view a specific web page, a client computer system specifies the URL for that web page in a request (e.g., a HyperText Transfer Protocol (“HTTP”) request). The request is forwarded to the web server that supports that web page. When that web server receives the request, it sends 10 the requested web page to the client computer system. When the client computer system receives that web page, it typically displays the web page using a browser. A browser is typically a special-purpose application program for requesting and displaying web pages.

Currently, web pages are often defined using HyperText Markup 15 Language (“HTML”) although other standards are on the horizon. HTML provides a standard set of tags that defines how a web page is to be displayed. When a user makes a request to the browser to display a web page, the browser sends the request to the server computer system to transfer to the client computer system an HTML document that defines the web page. When the requested 20 HTML document is received by the client computer system, the browser displays the web page as defined by the HTML document. The HTML document contains various tags that control the display of text, graphics, controls, and other features. The HTML document may contain URLs of other web pages available on that server computer system or on other server computer systems.

25 The World Wide Web portion of the Internet is especially conducive to conducting electronic commerce, and a host of other activities that individuals have previously performed manually or over the phone. One activity that has been difficult to transfer to the Internet or Word Wide Web has been voting. An electronic voting scheme must ensure the privacy of each voter, as well as provide 30 strict audit trails so that election officials or independent observers can verify no fraud has occurred. Furthermore, as with many electronic commerce techniques,

such an electronic voting scheme must be easy for voters to use. Ballot types must range from simple yes/no initiatives to complex multi-way candidate races allowing for the possibility of write-in candidates. The ballots must be tamper free, and must be sufficiently non-transitory, so that months after an election, the 5 ballots and results can be reviewed by some independent authority. To date, the inventors are unaware of any system that fulfills these requirements.

BRIEF DESCRIPTIONS OF DRAWINGS

The headings provided herein are for convenience only, and do not affect the scope or meaning of the claimed invention.

10 Figure 1 is a block diagram illustrating an environment for use with an embodiment of the invention.

Figure 2 is a block diagram illustrating one embodiment for permanently storing electronic ballots for use with the environment of Figure 1.

15 Figure 3 is a flow diagram showing steps performed by the embodiment of Figure 2.

Figure 4 is a block diagram illustrating an alternative embodiment for permanently storing electronic ballots for use with the environment of Figure 1.

DETAILED DESCRIPTION

20 Aspects of the invention overcome limitations of the prior art and provide numerous additional benefits. In one embodiment of the invention, ballots are permanently stored using a Write-Once, Read-Many (WORM) drive. This prevents anyone, such as election officials, hackers, etc., from erasing votes or altering ballots from an electronic "ballot box". The electronic ballot box is 25 formed as one or more web pages in an electronic "bulletin board" or voting website hosted by one or more web servers. Alternative embodiments employ other permanent data storage devices, as explained below.

The following description provides specific details for a thorough understanding of, and enabling description for, embodiments of the invention.

However, one skilled in the art will understand that the invention may be practiced without these details. In other instances, well known structures and functions have not been shown or described in detail to avoid unnecessarily obscuring the description of the embodiments of the invention.

5 Some of the detailed description provided herein is explicitly disclosed in the provisional patent applications; much of the additional material will be recognized by those skilled in the relevant art as being inherent in the detailed description provided in the provisional patent applications, or well known to those skilled in the relevant art. Those skilled in the relevant art can readily
10 implement aspects of the invention based on the detailed description provided in the provisional patent applications.

Figure 1 and the following discussion provide a brief, general description of a suitable computing environment in which aspects of the invention can be implemented. Although not required, embodiments of the invention will be
15 described in the general context of computer-executable instructions, such as routines executed by a general-purpose computer, such as a personal computer or web server. Those skilled in the relevant art will appreciate that aspects of the invention (such as for small elections) can be practiced with other computer system configurations, including Internet appliances, hand-held devices,
20 multiprocessor systems, microprocessor-based or programmable consumer electronics, network PCs, mini computers, cell phones, mainframe computers, and the like. Aspects of the invention can be embodied in a special purpose computer or data processor that is specifically programmed, configured or constructed to perform one or more of the computer-executable instructions explained herein.
25 The invention can also be practiced in distributed computing environments where tasks or modules are performed by remote processing devices, which are linked through a communications network, such as a Local Area Network (LAN), Wide Area Network (WAN), and the Internet. In a distributed computing environment, program modules or sub-routines may be located in both local and remote memory
30 storage devices.

Unless described otherwise, the construction and operation of the various blocks shown in Figure 1 and 2 are of conventional design. As a result, such blocks need not be described in further detail herein, as they will be readily understood by those skilled in the relevant art.

5 Referring to Figure 1, a suitable environment of system 100 includes one or more voter or client computers 102, each of which includes a browser program module 104 that permits the computer to access and exchange data with the Internet, including web sites within the World Wide Web portion 106 of the Internet. The voter computers 102 may include one or more central processing
10 units or other logic processing circuitry, memory, input devices (e.g., keyboards and pointing devices), output devices (e.g., display devices and printers), and storage devices (e.g., fixed, floppy, and optical disk drives), all well known but not shown in Figure 1. The voter computers 102 may also include other program modules, such as an operating system, one or more application programs (e.g.,
15 word processing or spread sheet applications), and the like. As shown in Figure 1, there are N number of voter computers 102, representing voters 1, 2, 3 . . . N .

A server computer system 108, coupled to the Internet or World Wide Web ("Web") 106, performs much or all of the ballot collection, storing and other processes. A database 110, coupled to the server computer 108, stores much
20 of the web pages and data (including ballots) exchanged between the voter computers 102, one or more voting poll computers 112 and the server computer 108. The server computer system 108, including the database 110, may employ security measures to inhibit malicious attacks on the system and to preserve the integrity of the ballots and other data stored therein.

25 The voting poll computer 112 is a personal computer, server computer, mini-computer, or the like, positioned at a public voting location to permit members of the public, or voters who may not have ready access to computers coupled to the Internet 106, to electronically vote under the system described herein. Thus, the voter computers 102 may be positioned at individual
30 voter's homes, where one or more voting poll computers 112 are located publicly or otherwise accessible to voters in a public election. The voting poll computer

112 may include a local area network (LAN) having one server computer and several client computers or voter terminals coupled thereto via the LAN to thereby permit several voters to vote simultaneously or in parallel.

Under an alternative embodiment, the system 100 may be used. In 5 the context of a private election, such as the election of corporate officers or board members. Under this embodiment, the voter computers 102 may be laptops or desktop computers of shareholders, and the voting poll computer 112 can be one or more computers positioned within the company (e.g., in the lobby) of the company performing the election. Thus, shareholders may visit the company to 10 access the voting poll computer 112 to cast their votes. One or more optional authority or organization computers 114 may also be coupled to the server computer system 108 via the Internet 106. The authority computers 114, in certain electronic voting schemes, each hold a key necessary to decrypt the tally of electronic ballots stored in the database 110. Threshold cryptographic systems 15 require that a subset t of the total number of authorities n (i.e., $t < n$) agree to decrypt the ballots, to thereby avoid the requirement that all authorities are needed for ballot decryption. The authority computers 114 may provide decryption shares based on their keys to the server computer system 108 after the voting period ends so that the server computer system may decrypt the tally results.

20 The server computer 108 includes a server engine 120, a web page management component 122, a database management component 124, as well as other components shown more clearly in Figure 2. The server engine 120 performs, in addition to standard functionality, performs one or more electronic voting protocols, such as the protocols described in U.S. Patent Application 25 No. _____, filed March 24, 2000, entitled "Multi-way Election Method and Apparatus," and assigned to the same assignee as this invention. Thus, the server engine 120 performs all necessary ballot transmission to authorized voters, ballot collection, verifying ballots (e.g., checking digital signatures and passing verification of included proofs of validity in ballots), vote aggregation, ballot decryption and/or vote tabulation.

The web page component 122 handles creation and display or routing of web pages such as an electronic ballot box web page, as described below. Voters and users may access the server computer 108 by means of a URL associated therewith, such as <http://www.votehere.net>, or a URL associated with the election, such as a URL for a municipality. The municipality may host or operate the server computer system 108 directly, or automatically forward such received electronic ballots to a third party vote authorizer who may operate the server computer system. The URL, or any link or address noted herein, can be any resource locator.

The web page management process 122 and server computer 108 may have secure sections or pages that may only be accessed by authorized people, such as authorized voters or system administrators. The server computer 108 may employ a secure socket layer ("SSL") and tokens or cookies to authenticate such users. Indeed, for small elections, or those where the probability of fraud is low (or results of fraud are relatively inconsequential), the system 100 may employ such simple network security measures for gathering and storing votes as explained below, rather than employing complex electronic encrypted ballots, as described in the above-noted patent application. Methods of authenticating users (such as through the use of passwords), establishing secure transmission connections, and providing secure servers and web pages are known to those skilled in the relevant art.

Referring to Figure 2, a more detailed representation of the server computer system 108 is shown. The server computer system 108 includes a router 202 coupled between the Internet 106 and a firewall 204. The router 202 acts as an interface between the Internet 106 and the server computer system 108. The router 202 receives incoming electronic ballots or votes produced by the voter computers 102 or voting poll computer 112, and routes them through the firewall 204 to a web-load balancing system 206.

The firewall 204 protects the server computer system 108 from attacks or security breaches directed at the system from the Internet 106. Any of various known firewall systems may be employed, such as those employing

screened subnet architecture (e.g., packet filtering), and multi-homed host architecture (e.g., application gateway or dedicated proxy methods), although any of the many known firewall architectures may be employed.

The web-load balancing system 206 balances load on several web server computers 208 (three of which are shown in Figure 2). Load balancing is a technique well known in the art for distributing the processing load between two or more computers, to thereby more efficiently process instructions and route data. In the present context, the web-load balancing system 206 helps distribute received electronic ballots evenly between the web servers 208, which can be particularly important at peak traffic times.

As shown in Figure 2, each of the web servers 208 include internally or have coupled thereto write-once, read-many (WORM) drives 210. As explained more fully below, the WORM drives 210 permanently store received electronic ballots. Thus, in addition to the database 110 which stores the ballots for rapid access and processing by the web servers 208, the WORM drives 210 permanently store such ballots in the event of a catastrophic fault, or to later verify election results, as noted below. As shown by the broken lines in Figure 2, the web load balancing device 206 may directly route received ballots to the WORM drives 210 (as opposed to having such ballots first being directed to the web servers 208).

The web-load balancing system 206 acts as an interface to the WORM drives 210 to provide load balancing for such drives so that all electronic ballots are permanently stored on the WORM drives in an efficient manner, particularly during times of peak traffic, and to overcome relatively slow write times (as compared to, for example, random access memory (RAM) write times). Each of the web servers 208 executes a software enabled application programming interface (API) running as a service thereon to enable writing of the electronic ballots onto the associated WORM drive 210. APIs for interfacing an application program such as the ballot collection and vote tallying process noted above and the writing of received ballots to the WORM drives 210 is similar to conventional APIs for permitting application programs for writing data to WORM drives or

other similar drives. Several web servers 208 and WORM drives 210 are employed for not only efficient load balancing of received web traffic and/or electronic ballots, but also for redundancy and fault tolerance reasons. Indeed, while only a single router 202, firewall 204 and web-load balancing system 206 are shown in Figure 2, the server computer system 108 may employ two or more such devices/systems to further improve fault tolerance for the system. To further improve processing efficiency, the web servers 208 may employ cryptographic accelerator cards or math coprocessors not shown to expedite cryptographic functions when the server computer system 108 execute cryptographically complex electronic elections. Likewise, the voting poll computer 112 and/or voter computers 102 can employ such cryptographic accelerator cards or math coprocessors for similar reasons.

Any of several known WORM drives may be employed, such as Model No. CMO R540 MO, by Sony Corporation, Model No. HP5200ex SureStore, by Hewlett Packard, and Model No. T6-5200, by Maxoptix. These drives typically employ a 5.2 inch (13.2 centimeter) diameter, optical disk or cartridge, enhanced polycarbonate-type continuous composite WORM (CCW), having up to 5.2 Gigabytes of storage. Once data, such as electronic ballots, has been written to the optical disks in the WORM drives 210, the data may not later be erased or altered. In other words, such WORM drives 210 permit data to be permanently stored thereon once, and then thereafter read therefrom numerous times.

Other permanent data storage devices are possible. Digital Versatile Disk (DVD) drives may be used instead of the WORM drives 210. DVD drives offer wide support on various computing platforms, as well as high capacity, wide feature set, numerous drivers supporting such disks, low cost, and the like. CD-Write once media may also be employed, but may suffer from low memory capacity when used with large elections employing encrypted ballots.

Other permanent data storage media and associated data storage devices may be used, and may be desirable in certain elections. For example, the web servers 208 may be coupled to one, or a bank of, smart cards, printed circuit

boards or cartridges containing programmable read-only memory (PROM), electronically programmable read-only memory (EPROM), and the like. Such memory may provide faster write times than WORM drives, but may be less tamper resistant and more expensive, particularly for elections with numerous 5 voters and large ballots. Other computer-readable media may include magnetic disk drives, Bernoulli cartridges, and flash memory cards, if sufficient safeguards are employed (both hardware and software) to ensure that ballots stored thereon are tamper proof and not subject to fraud once ballots had been written thereto.

Under one embodiment, the server computer system 108 provides a 10 website or "bulletin board" to which each voter posts his or her digitally signed electronic ballot. The server computer system 108 permanently stores each ballot in the database 110, so that ballots may not be altered or erased, as described herein. Once the predetermined polling period ends ("the polls close"), the web server computer system 108 verifies each ballot and aggregates or tallies them to 15 produce a final tally, although verification, and some or all portions of ballot aggregation, decryption and tallying can be performed as ballots are received (or "on the fly").

Referring to Figure 3, a process 300 performed by the server 20 computer system 108 and voting organization providing such system is shown. To illustrate the processes 300 for gathering and storing electronic ballots, each component or step is generally described as a single function performed by the server computer system 108 (or authority employing such system). One skilled in the relevant art will appreciate that each of these components or steps may be implemented as several separate routines or subroutines.

25 In step 302, the server computer system 108 provides electronic ballots to authorized voters. Voters may be authorized in any number of processes, such as those described in U.S. Patent Application No. _____, filed March 24, 2000, entitled "Method, Article and Apparatus for Registering Registrants, Such As Voter Registrants" and assigned to 30 the assignee of the present invention. Each electronic ballot includes all

predetermined voting issues, instructions for voting, and any relevant cryptographic keys or processes.

Additionally, each electronic ballot includes a digital signature provided by the server computer system 108. Thus, voters who receive such 5 ballots may check the digital signature to ensure that the ballot has not been corrupted or altered.

Under step 302, the electronic ballots may be emailed to each of the authorized voters. Under this method, the database 110 includes the email 10 addresses, URLs, links or other logical addresses for the voter computers 102 and voting poll computer 112. The server computer system 108 then automatically retrieves each logical address and forwards the appropriate electronic ballot to each address. Alternatively, the server computer system 108 may provide a web 15 page to be accessed by the voting computers 102 and voting poll computer 112. By accessing such web page, and proving authentication of the relevant voter, the voter may then download from the server computer system 108 an electronic 20 ballot. These two methods of electronic ballot distribution represent server initiated and client initiated distribution methods; of course, many other similar methods may be employed whereby the server computer system 108 forwards electronic ballots to authorized users, or where the voter computers 102 and voting poll computer 112 request electronic ballots.

In step 304, the server computer 108 receives electronically signed 25 ballots from the voters. In one embodiment, the server computer system 108 provides the above-noted web page bulletin board that allows each voter to post his or her ballot thereto during a predetermined voting period. Of course, other methods for receiving electronic ballots are possible, including email, wireless data transmission (e.g., via cell phone or portable/wearable computer), and the like. The server computer 108 may provide a digitally signed receipt to the voter 30 recognizing receipt of the voter's electronic ballot. Furthermore, the server computer 108 may first provide such receipt to one or more of the authority computers 114 who in turn add their digital signatures before forwarding the receipt to the voter.

After the predetermined voting period ends, the server computer 108 no longer permits additional ballots to be received and written to the WORM drive 210. Under an alternative embodiment, the server computer system 108 continues to collect additional ballots after the predetermined voting period, but 5 flags each ballot as being late or otherwise provides some indication about when such ballots were received. The web server computer 208, under this alternative embodiment, does record such late ballots via the WORM drives 210.

In step 306, the web servers 208 in the server computer system 108 write each received ballot to the WORM drives 210 or other permanent data 10 storage media devices. In general, it is desirable to write each ballot received under step 304 immediately to one of the WORM drives 210 under step 306. Under an alternative embodiment, the server computer system 108 may employ 15 solid state memory (e.g., RAM) or other electronic memory buffers to buffer and hold electronic ballots temporarily before being written to one of the WORM drives 210. Such electronic buffers are particularly useful during peak traffic times, however, may suffer from possible security shortcomings in that a fraudulent voting organization could tamper with electronic ballots, when in the buffer, before they are written to the WORM drives 210.

In step 308, the server computer system 108 verifies each received 20 ballot. The verification can include checking the digital signature of each received ballot, and verifying the validity of each ballot, such as verifying correct hash function output and/or proofs of validity, such as under zero knowledge proofs. Such verification can be performed as the server computer system 108 sequentially reads each ballot previously written to the WORM drives 210. 25 Alternatively, the server computer system 108 can perform some or all of such verification of received ballots before step 306 (before they are written to the WORM drives 210). For example, the server computer system 108 can verify the digital signature or compute the hash function of each ballot before writing it to the WORM drives 210. If the digital signatures do not verify or the computer hash function results do not match, the server computer system 108 may discard 30 such ballots, and not write them to the WORM drives 210. However, third party

voting verification authorities may request that all received ballots be permanently stored before any unauthorized ballots are discarded.

In step 310, the server computer system 108 aggregates the stored ballots and decrypts the results, with a threshold number of authorities if such an 5 encryption protocol is employed. Ballot authorization and decryption under a threshold number of authorities is described in greater detail in the Multi-Way Election Method and Apparatus application noted above.

In step 312, the voting organization providing the server computer system 108 may provide the storage data to a voter verification authority. For 10 example, the voting organization may provide one or more WORM disks from the WORM drives 210 to a third party organization who verifies that no fraud had occurred during the vote or ballot tabulation. Any method of physically transferring the WORM disks to such a third-party vote verifying organization may be employed, including courier services.

15 Under an alternative embodiment, the server computer system 108 may employ a one-way hash function or simple error correction/detection technique (e.g., cyclic redundancy check (CRC)) to the data, or groups of data stored on the WORM disk. The server computer system 108, at predetermined times, or after a predetermined number of electronic ballots have been received, 20 perform such a hash function or other method to provide an additional level of security and verification to ballots stored by the WORM drives 210. The results of the hash function are then likewise stored by the WORM drive, and can be presented to and verified by the third-party voting verification authority.

In step 314, the voting organization running the server computer 25 system 108 and/or third-party voting verification authority may destroy the WORM disks after a predetermined time period. Many elections require that all ballots be saved or stored for a predetermined time period during which third parties may challenge or review election results to ensure that no fraud occurred. After such predetermined time period, however, the ballots typically must be 30 destroyed. Therefore, the WORM disks may then be destroyed in step 314, to thereby effectively eliminate all electronic ballots. Of course, the voter computers

102 may each have stored thereon, their own ballots, but this option is left to each voter.

Under one embodiment of the invention, which employs the protocols described in the above-noted patent application, electronic ballots may 5 be digitally signed by each authorized voter and posted by the voters to an area on a bulletin board or website representing a "ballot box." Ballots are encrypted by the voters but never decrypted. Multi-way elections are possible using both discrete log, elliptic curve and general group cryptosystems, all of which employ homomorphic properties to allow ballots to be combined to produce 10 encrypted tallies. This multi-way election scheme ensures universal verifiability since any third party can see who voted without seeing how they voted and duplicate the combination of the encrypted ballots to obtain the encrypted tally. Ballots are accompanied with zero-knowledge proofs of validity to ensure that a 15 voted ballot includes only allowable options, without leaking any information about which ballot option the voter chose. Such proofs are non-interactive and all received ballots are automatically stored permanently by the WORM drives 210. The encrypted tallies are decrypted by t of n authorities without reconstructing the authorities' private key, using threshold encryption techniques. The decryption 20 protocol requires a zero-knowledge proof which ensures that the correct ciphertext (ballot) has been decrypted using the private-key share corresponding to the authorities' group public-key. Further, compromise of the voter privacy would require a conspiracy of at least t of the n number of authorities.

The server computer system 108, with the WORM drives 210 or other permanent data storage devices, are useful for not only storing electronic 25 ballots, but also for registering preregistered write-in candidates for elections, and other data for write-in candidates and votes. Under the multi-way election method and apparatus application noted above, a write-in candidate submits his or her name, ballot or precinct identifier and a race identifier. The server computer system 108 generates a candidate number for the identified race and computes a 30 unique encryption generator. The candidate's name, ballot identifier, race identifier, candidate number and generator are stored by the WORM drive 210.

Before the beginning of the election, registration of new write-in candidates is closed, and information for all write-in candidates is read from the WORM drive 210 by the server computer 108 and added to the appropriate electronic ballots before such ballots are distributed to voters. All received ballots are then stored 5 on the WORM drive 210, together with any and all votes for preregistered write-in candidates.

Under an alternative method for write-in candidates described in the above application, a database is created containing a record for each person eligible to hold any office appearing on the ballot. The record contains the 10 person's name, unique identifier and an encryption generator. For any given race, the voter may fill in the name of a write-in candidate on the electronic ballot. The server computer system 108 then queries the database for that name, and if a match is found, the unique identifier and any necessary encryption data are used to form the vote for that candidate on the electronic ballot. The WORM drive 210 15 may be used to create a permanent record of such database for all eligible people to hold office on a given ballot. This permanent record could then be later reviewed by a third-party vote verification authority to ensure that all relevant names were included in the database.

Referring to Figure 4, an alternative embodiment of the invention is 20 depicted as a system 400. As shown in Figure 4, the web server computers 208 are coupled directly to the internet 106, such as by means of only SSL and TCP/IP ports. Thus, the web servers 208 have only a limited command set and are thus more secure than platforms coupled to the internet by means of a router or other high functionality/command set devices.

25 The web servers 208 are coupled to an array of WORM drives 210 by means of a distributed file server 402. A distributed file server or system is a type of file system in which the file system itself manages and transparently locates pieces of information (e.g. ballots) from remote files and distributes files across a network, such as the LAN effectively formed by the web servers, WORM 30 drives and distributed file server shown in Figure 4. The distributed file server 402 also manages read and write functions to the WORM drives 210 and database

110. The distributed file server 402 may be a process running on each, or one of, the web servers 208, or on a separate hardware device. Indeed, one of the web servers 208, WORM drives 210, and the database 110 may be enclosed within a single box to form a "vote engine" that may be connected directly to the Internet 5 106 as a stand alone product.

The distributed file server 402 receives ballots from the web servers 402 and determines which of several WORM drives 210 to instruct to write the ballot. The distributed file server 402 also stores the received ballots in the database 110 for rapid access and rapid write-time with respect to the web servers 10 208. When one of the web servers 208 wishes to retrieve one of the ballots or some other file, the request is provided to the distributed file server 402, which in turn identifies where the ballot or desired file is stored, retrieves such ballot/file, and provides it to the web server.

As shown in Figure 4, one of the authority computers 114 also 15 includes a WORM drive 210 coupled thereto. Under the embodiment described above where the authority computers receive and digitally sign ballot receipts for the voter computer 102 (recognizing that the voter's electronic ballot has been received), the authority computer may store such receipts. To enhance data integrity, such received receipts may be stored in the WORM drive 210. Thus, the 20 authority computer can ensure that the web server computers 208 have not eliminated any ballots from the final tally. Of course, the authority computer 114 may receive and store on the WORM drive 210 other information, including ballots that may be forwarded thereto, and the like.

One skilled in the art will appreciate that the concepts of the 25 invention can be used in various environments other than the Internet. For example, the concepts can be used in an electronic mail environment in which electronic mail ballots or forms are processed and stored. In general, a web page or display description (e.g., the bulletin board) may be in HTML format, email format, or any other format suitable for displaying information (including character/code based formats, bitmapped formats and vector based formats). 30 Also, various communication channels, such as local area networks, wide area

networks, or point-to-point dial-up connections, may be used instead of the Internet. The various transactions may also be conducted within a single computer environment, rather than in a client/server environment. Each voter or client computer may comprise any combination of hardware or software that 5 interacts with the server computer or system. These client systems may include television-based systems, Internet appliances and various other consumer products through which transactions can be performed.

In general, as used herein, a "link" refers to any resource locator identifying a resource on the network, such as a display description of a voting 10 authority having a site or node on the network. In general, while hardware platforms, such as voter computers, terminals and servers, are described herein, aspects of the invention are equally applicable to nodes on the network having corresponding resource locators to identify such nodes.

Unless the context clearly requires otherwise, throughout the 15 description and the claims, the words 'comprise', 'comprising', and the like are to be construed in an inclusive sense as opposed to an exclusive or exhaustive sense; that is to say, in the sense of "including, but not limited to". Words using the singular or plural number also include the plural or singular number, respectively. Additionally, the words "herein", "hereunder", and words of similar import, when 20 used in this application, shall refer to this application as a whole and not to any particular portions of this application.

The above description of illustrated embodiments of the invention is not intended to be exhaustive or to limit the invention to the precise form disclosed. While specific embodiments of, and examples for, the invention are 25 described herein for illustrative purposes, various equivalent modifications are possible within the scope of the invention, as those skilled in the relevant art will recognize. The teachings of the invention provided herein can be applied to other record storage systems, not necessarily the electronic voting system described above.

30 The various embodiments described above can be combined to provide further embodiments. All of the above references and U.S. patents and

applications are incorporated by reference. Aspects of the invention can be modified, if necessary, to employ the systems, functions and concepts of the various patents and applications described above to provide yet further embodiments of the invention.

5 These and other changes can be made to the invention in light of the above detailed description. In general, in the following claims, the terms used should not be construed to limit the invention to the specific embodiments disclosed in the specification and the claims, but should be construed to include all ballot or record storage systems that operate under the claims to provide a
10 method for permanently storing such data. Accordingly, the invention is not limited by the disclosure, but instead the scope of the invention is to be determined entirely by the claims.

CLAIMS

1 1. An electronic voting system for use with a computerized
2 network, comprising:

3 a plurality of voting computers coupled to the computerized network,
4 wherein each voting computer provides an electronic encrypted ballot representing at
5 least one vote;

6 a server computer system coupled to the computerized network,
7 wherein the server computer system includes:

8 at least one server computer for receiving the plurality of
9 electronic ballots from the plurality of voting computers, performing at least
10 one cryptographic operation relative to the plurality of electronic ballots, and
11 determining a tally of the votes; and

12 a write-once, read-many data storage device coupled to the
13 server computer and having a computer-readable medium therein, wherein the
14 server computer and data storage device are configured to permanently write
15 the plurality of received electronic ballots to the computer-readable medium.

1 2. The system of claim 1, further comprising:
2 at least one voting poll computer coupled to the computerized network
3 and providing another plurality of electronic encrypted ballots to the server computer
4 system;
5 at least one authority computer coupled to the computerized network
6 that provides at least one cryptographic key for decrypting at least a portion of the
7 plurality of electronic ballots and the another plurality of electronic ballots; and
8 wherein the server computer system includes at least one router coupled
9 to the computerized network, and at least one firewall coupled between the router and
10 the server computer.

1 3. The system of claim 1, further comprising:
2 at least one voting poll computer coupled to the computerized network,
3 wherein the voting poll computer is coupled to a plurality of additional terminals over
4 a network to receive, and provide to the server computer system, another plurality of
5 electronic encrypted ballots.

1 4. The system of claim 1 wherein the computerized network
2 includes the World Wide Web, wherein each of the plurality of voting computers
3 include a web browser program, and wherein the server computer system includes:

4 at least two web server computers, each having at least one of
5 the data storage devices, wherein at least one of the web server computers
6 provides a ballot box web page for the plurality of voting computers to post
7 their respective electronic ballots thereto, and

8 a load balancing and fault tolerance system coupled between the
9 World Wide Web and the two web server computers, wherein the load
10 balancing and fault tolerance system is configured to provide substantially
11 equal numbers of the plurality of electronic ballots to the two web servers and

12 data storage devices, and to detect for and reroute received electronic ballots if
13 one of the two web server computers suffers a fault.

1 5. The system of claim 1 wherein the computer-readable medium
2 in the data storage device is a removable optical disk.

1 6. The system of claim 1 wherein the plurality of voter computers
2 include at least one palm-sized computer, cell phone, wearable computer, interactive
3 television terminal or Internet appliance.

1 7. A computer system for receiving a plurality of electronic ballots
2 over a network, comprising:

3 at least one server computer for receiving the plurality of
4 electronic ballots from the network, and performing at least one operation
5 relative to the plurality of electronic ballots; and

6 a permanent data storage device coupled to the server computer
7 and having a computer-readable medium, wherein the server computer and
8 data storage device are configured to write the plurality of received electronic
9 ballots to the computer-readable medium in an unalterable fashion, and
10 wherein the electronic ballots may be read from the computer-readable
11 medium thereafter.

1 8. The system of claim 7 wherein the electronic ballots are
2 encrypted and represent votes from a plurality of voters, wherein at least one
3 authority computer coupled to the network provides at least one cryptographic key to
4 the server computer for decrypting at least a tally from the plurality of electronic
5 ballots, and wherein the system further comprises:

6 at least one router coupled to the computerized network, and
7 at least one firewall coupled between the router and the server
8 computer.

9
1 9. The system of claim 7 wherein the network includes the World
2 Wide Web, and wherein the server computer system includes:

3 at least two web server computers coupled to the World Wide
4 Web;

5 at least two data storage devices coupled respectively to the two
6 web server computers, wherein at least one of the web server computers
7 provides a ballot box web page for receiving the electronic ballots.

1 10. The system of claim 7 wherein the server computer system
2 includes:

3 at least two server computers, each having one of the data
4 storage devices, and

5 a load balancing system coupled between the network and the
6 two server computers, wherein the load balancing system is configured to
7 distribute the plurality of electronic ballots to the two servers, the data storage
8 devices, or both.

9
1 11. The system of claim 7 wherein the data storage device is a write-
2 once, read-many (WORM) drive.

1 12. The system of claim 7 wherein the data storage device is a CD-R
2 drive.

1 13. The system of claim 7 wherein the data storage device is a
2 digital versatile disk (DVD) drive.

1 14. The system of claim 7 wherein the data storage device is a
2 removable structure, and wherein the computer-readable medium includes, secured to
3 the structure, programmable read only memory (PROM) or electronically
4 programmable read only memory (EPROM).

1 15. The system of claim 7 wherein the server computer receives at
2 least some of the plurality of electronic ballots from at least one palm-sized
3 computer, cell phone, wearable computer, interactive television terminal or Internet
4 appliance.

1 16. The system of claim 7 wherein the server computer performs a
2 hash or error detection operation on at least one set of the electronic ballots stored by
3 the data storage device, and wherein the data storage device stores a result of the
4 operation on the computer-readable medium.

1 17. The system of claim 7 wherein the server computer performs an
2 authentication or verification operation on at least one set of the received electronic
3 ballots and does not cause the data storage device to store those electronic ballots that
4 fail the authentication or verification operation.

1 18. The system of claim 7 wherein the server computer adds a late
2 flag to at least one set of the plurality of electronic ballots stored by the data storage

3 device, wherein the late flag indicates that the set of electronic ballots were received
4 outside of a predetermined time period.

5

1 19. The system of claim 7 wherein the server computer is configured
2 to receive write-in candidate data and wherein the server computer and data storage
3 device are configured to write the write-in candidate date to the computer-readable
4 medium in an unalterable fashion.

1 20. The system of claim 7, further comprising: another permanent
2 data storage device having a computer-readable medium for storing at least some of
3 the plurality of received electronic ballots thereto; and

4 a distributed file server communicating with the permanent data storage
5 device and the another permanent data storage device, and which receives the
6 electronic ballots and determines to which of the data storage devices to route the
7 received electronic ballots.

8

1 21. In an electronic voting system having a data processing device
2 coupled to a network for receiving a plurality of electronic ballots, an apparatus
3 comprising:

4 a permanent data storage device coupled to the data processing device
5 and having a computer-readable data storage medium, wherein the data storage
6 device is configured to receive the plurality of received electronic ballots from the
7 data processing device and to write the plurality of received electronic ballots to the
8 computer-readable medium in an unalterable fashion, and wherein the data
9 processing device may read the electronic ballots from the computer-readable
10 medium thereafter, but not alter or delete any of the electronic ballots.

11

1 22. The apparatus of claim 21 wherein the electronic ballots are
2 encrypted and represent votes from a plurality of voters, wherein the network
3 includes the World Wide Web having a virtual ballot box for receiving the plurality

4 of electronic ballots, wherein the computer-readable data storage medium is an
5 optical disk and wherein the optical disk forms a permanent record for electronic
6 ballots posted to the virtual ballot box.

1 23. The apparatus of claim 21 wherein the electronic ballots are
2 encrypted and wherein the permanent data storage device stores the encrypted
3 electronic ballots.

1 24. The apparatus of claim 21 wherein the data storage device is a
2 write-once, read-many (WORM) drive.

1 25. The apparatus of claim 21 wherein the data storage device is a
2 CD-R drive.

1 26. The apparatus of claim 21 wherein the data storage device is a
2 digital versatile disk (DVD) drive.

1 27. The apparatus of claim 21 wherein the data storage device is a
2 removable structure, and wherein the computer-readable medium includes, secured to
3 the structure, programmable read only memory (PROM) or electronically
4 programmable read only memory (EPROM).

1 28. The apparatus of claim 21 wherein the data processing device
2 performs a hash or error detection operation on at least one set of the plurality of
3 electronic ballots stored by the data storage device, and wherein the data storage
4 device stores a result of the operation on the computer-readable data storage medium.

1 29. The apparatus of claim 21 wherein the data processing device
2 adds a late flag to at least one set of the plurality of electronic ballots stored by the

3 data storage device, wherein the late flag indicates that the set of electronic ballots
4 were received outside of a predetermined time period.

5

1 30. A computer-readable medium for storing a computer readable
2 data structure, comprising:

3 a write-once, read-many computer readable medium having written
4 thereto a plurality of encrypted electronic ballots from a plurality of voters, wherein
5 each encrypted electronic ballot represents at least one vote from one of the plurality
6 of voters, wherein a data processing device may read the plurality of encrypted
7 electronic ballots from the write-once, read-many computer-readable medium, but not
8 alter or delete any of the encrypted electronic ballots.

1 31. The apparatus of claim 30 wherein the data processing device is
2 an authority computer, and wherein the permanent data storage device stores digitally
3 signed receipts indicating receipt of received electronic ballots.

1 32. The computer-readable medium of claim 30 wherein the write-
2 once, read-many computer readable medium is a write-once, read-many (WORM)
3 optical disk.

1 33. The apparatus of claim 30, further comprising a distributed file
2 system communicating with the permanent data storage device, which receives the
3 electronic ballots from the data processing device.

1 34. The computer-readable medium of claim 30 wherein the write-
2 once, read-many computer readable medium is a CD-R disk.

1 35. The computer-readable medium of claim 30 wherein the write-
2 once, read-many computer readable medium is a digital versatile disk (DVD) disk.

1 36. The computer-readable medium of claim 30 wherein the write-
2 once, read-many computer readable medium is a removable structure having secured
3 thereto programmable read only memory (PROM) or electronically programmable
4 read only memory (EPROM).

1 37. An electronic voting method, comprising:
2 receiving a plurality of electronic ballots from a plurality of
3 voters from a network;
4 performing at least one operation relative to the plurality of
5 electronic ballots; and
6 writing each of the plurality of received electronic ballots to a
7 computer-readable medium in an unalterable fashion.

1 38. The method of claim 37 wherein receiving a plurality of
2 electronic ballots includes receiving encrypted electronic ballots representing votes
3 from a plurality of voters, and wherein the method further comprises:
4 distributing, over the network, a plurality of initial electronic ballots to
5 the plurality of voters;
6 receiving at least one cryptographic key from at least one authority for
7 decrypting at least a portion of the plurality of electronic ballots;
8 decrypting at least a tally of the electronic ballots based on the received
9 key or keys; and
10 providing the computer-readable medium to a third party verifier after
11 decrypting.

12

1 39. The method of claim 37 wherein receiving a plurality of
2 electronic ballots includes receiving the electronic ballots over the World Wide Web,
3 and wherein the method further comprises:

4 providing a ballot box web page for receiving the electronic
5 ballots.

1 40. The method of claim 37 wherein receiving a plurality of
2 electronic ballots includes receiving over the network at least some of the plurality of
3 electronic ballots from at least one palm-sized computer, cell phone, wearable
4 computer, interactive television terminal or Internet appliance.

1 41. The method of claim 37, further comprising:

2 performing a hash or error detection operation on at least one set of the
3 electronic ballots; and

4 storing a result of the operation on the computer-readable medium.

1 42. The method of claim 37, further comprising performing an
2 authentication or verification operation on the plurality of received electronic ballots.

1 43. The method of claim 37, further comprising:

2 adding a late flag to at least one set of the plurality of electronic ballots,
3 wherein the late flag indicates that the set of electronic ballots were received outside
4 of a predetermined time period; and

5 writing the set of electronic ballots to the computer-readable medium
6 with associated flags.

7

44. The method of claim 37 wherein the instructions are performed in the order of receiving a plurality of electronic ballots, performing at least one cryptographic operation, and writing each of the plurality of received electronic ballots..

5

45. A computer-readable medium storing instructions for instructing a computer coupled to a network, the instructions comprising:

receiving a plurality of electronic ballots from a plurality of voters from the network; and

10

writing each of the plurality of received electronic ballots to a computer-readable medium in an unalterable fashion.

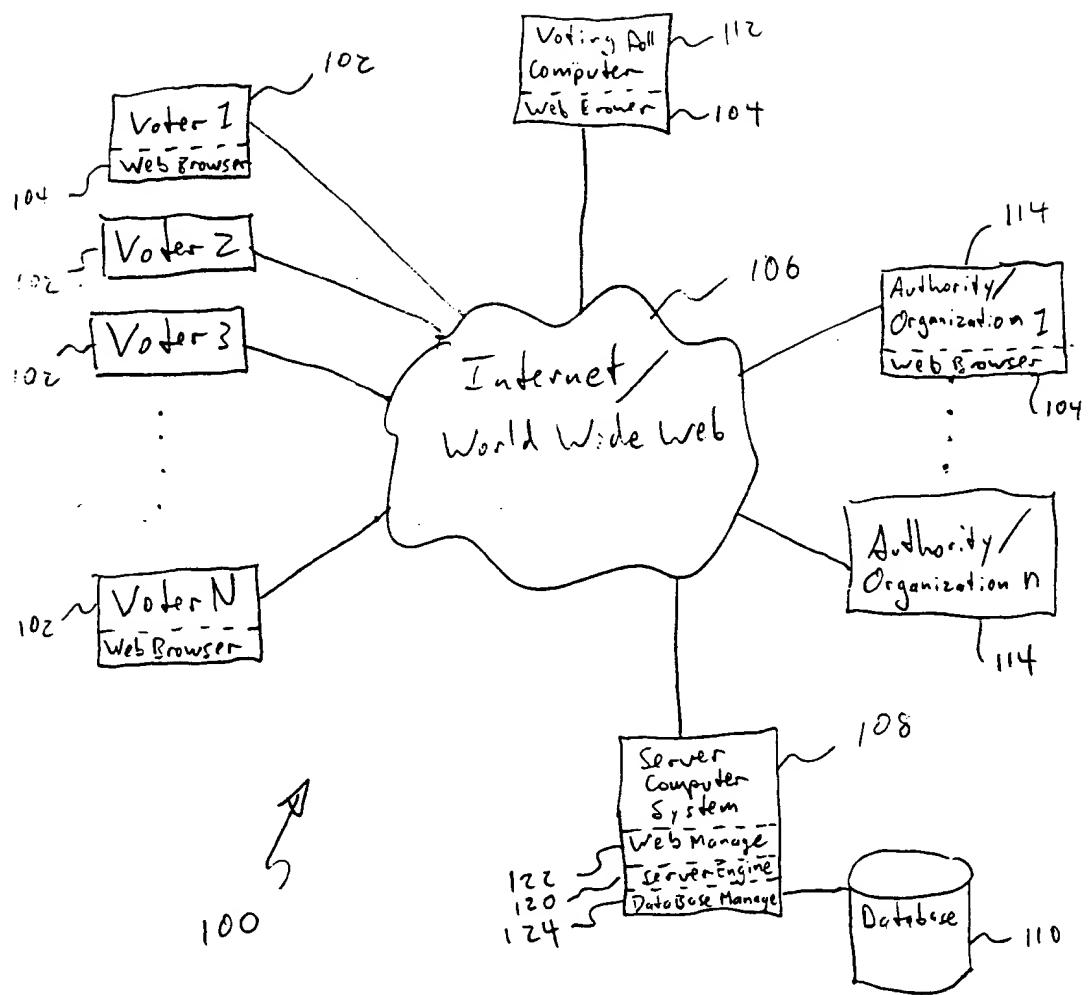
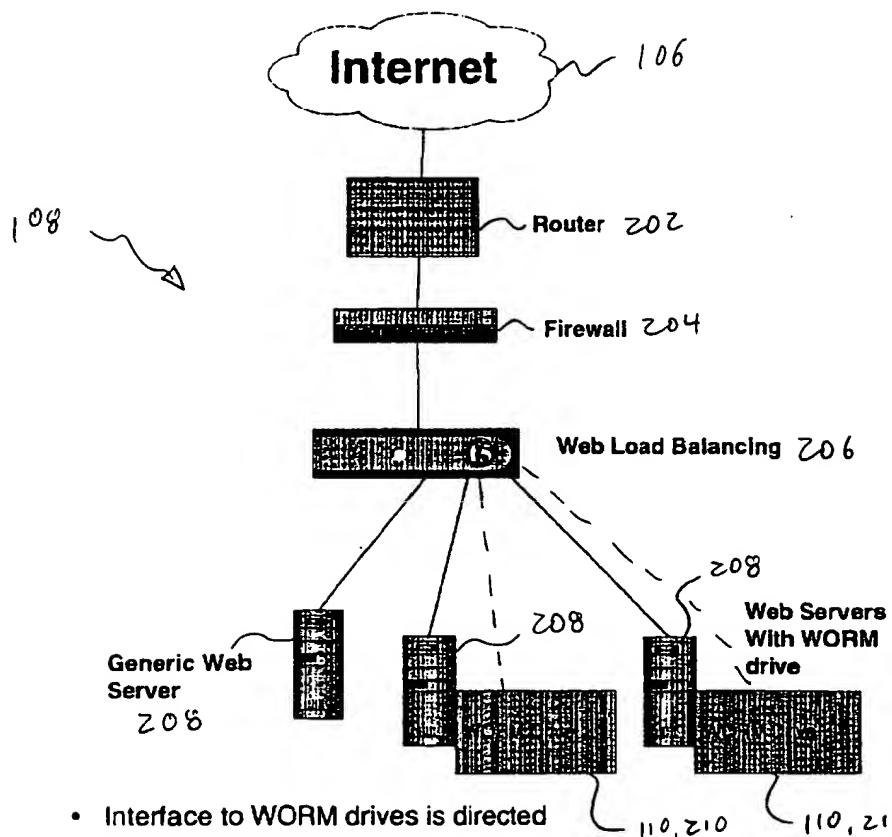


FIG 1



- Interface to WORM drives is directed through web load balancing device to provide load balancing for WORM service.
- Interface to WORM drives is via a software API running as a service on the WORM enabled Web servers.

Fig 2

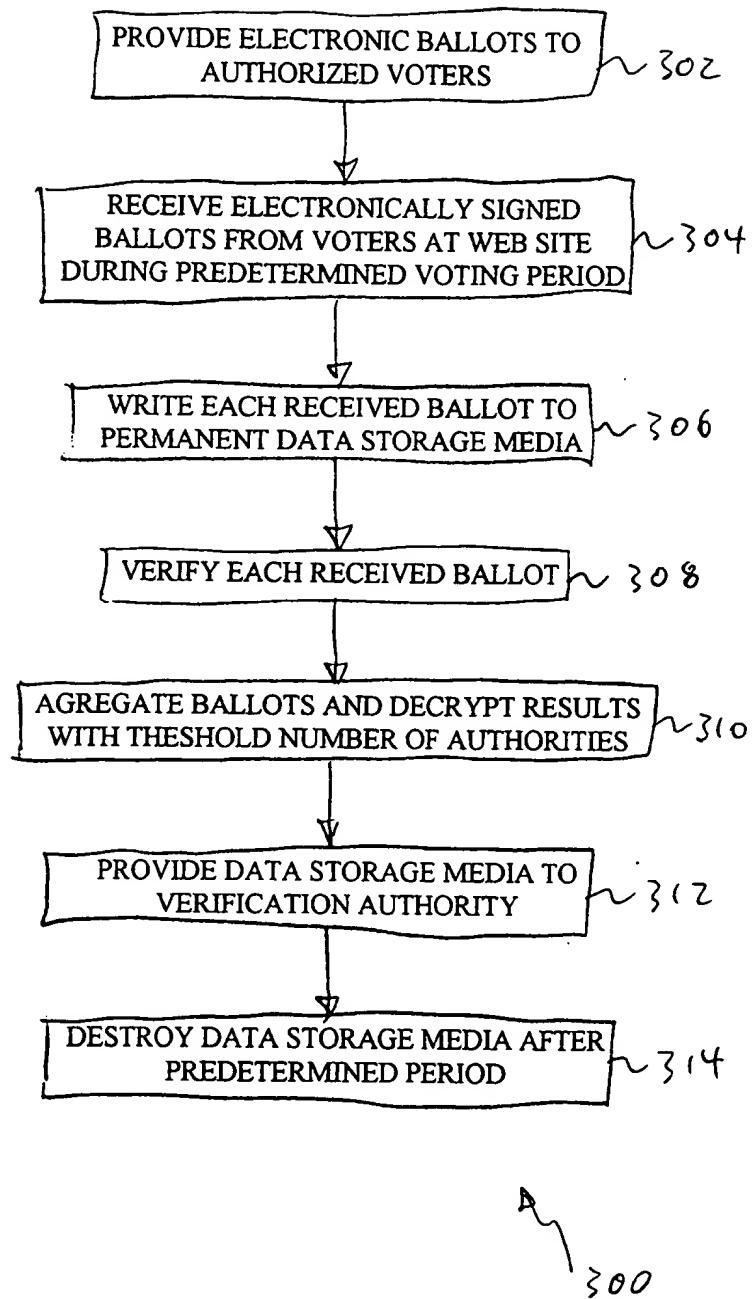


FIG 3

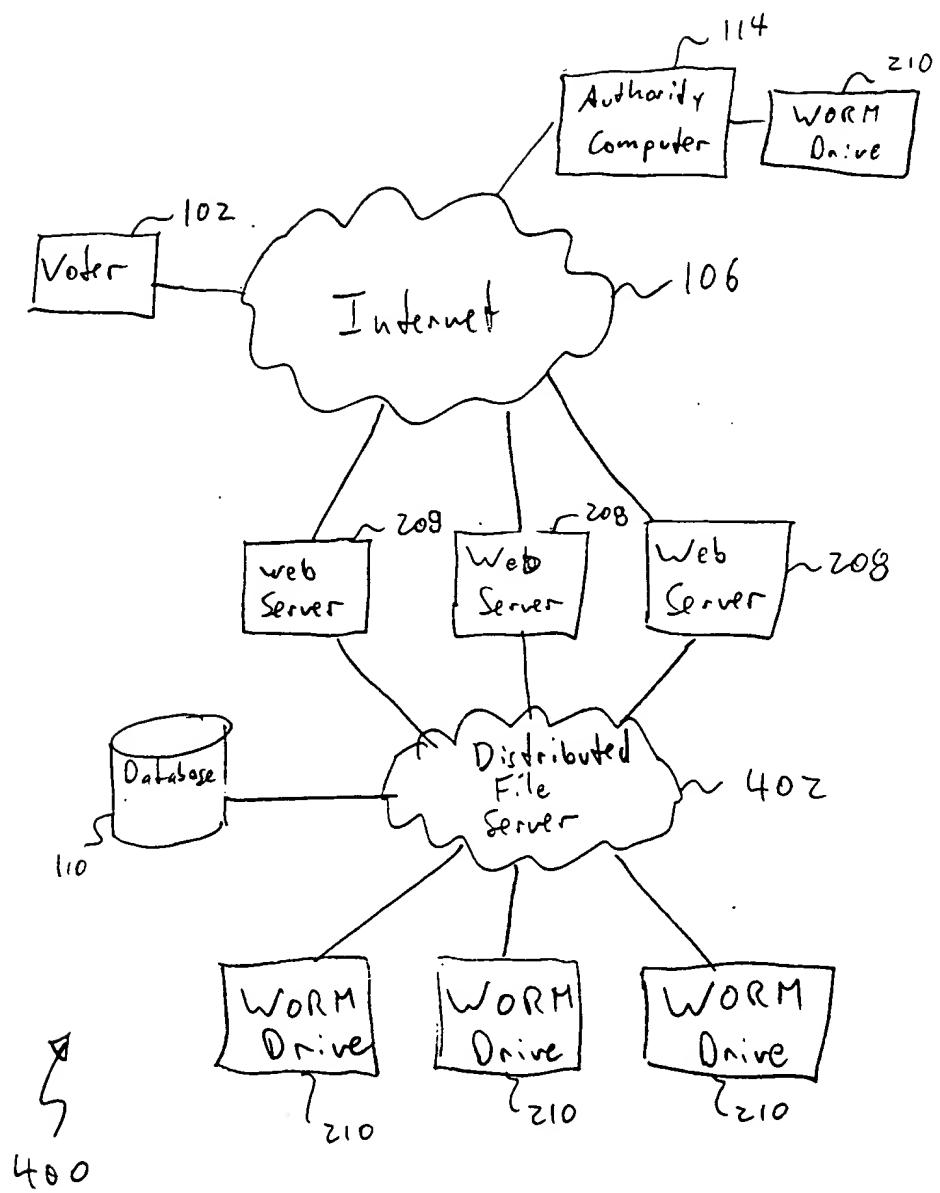


FIG 4

CORRECTED VERSION

(19) World Intellectual Property Organization
International Bureau(43) International Publication Date
29 March 2001 (29.03.2001)

PCT

(10) International Publication Number
WO 01/022200 A2(51) International Patent Classification⁷: G06FADLER, Jim [US/US]; Suite 250, 3101 Northup Way,
Bellevue, WA 98004 (US).

(21) International Application Number: PCT/US00/07986

(74) Agents: DALEY-WATSON, Christopher, J. et al.;
Perkins Coie LLP, Suite 4800, 1201 Third Avenue, Seattle,
WA 98101-3099 (US).

(22) International Filing Date: 24 March 2000 (24.03.2000)

(81) Designated States (national): AE, AL, AM, AT, AU, AZ,
BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE,
ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE,
KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG,
MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE,
SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN,
YU, ZA, ZW.

(25) Filing Language: English

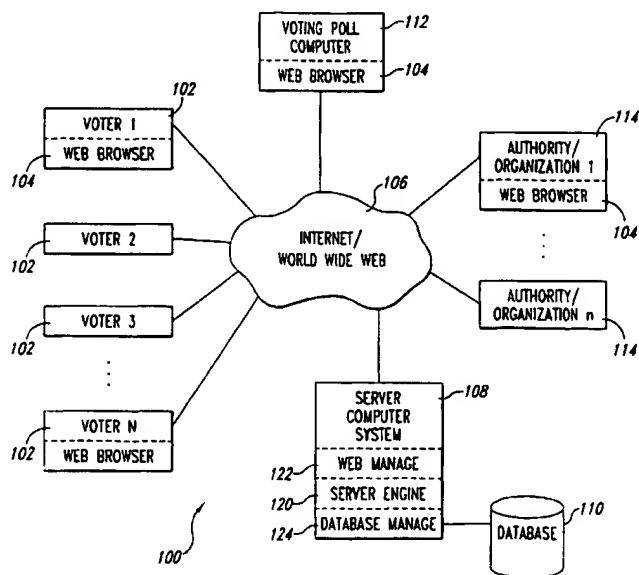
(26) Publication Language: English

(30) Priority Data:

60/126,080 25 March 1999 (25.03.1999) US
60/149,621 16 August 1999 (16.08.1999) US(84) Designated States (regional): ARIPO patent (GH, GM,
KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent
(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent
(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU,
MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM,
GA, GN, GW, ML, MR, NE, SN, TD, TG).(71) Applicant (for all designated States except US): VOTE-
HERE, INC. [US/US]; Suite 250, 3101 Northup Way,
Bellevue, WA 98004 (US).

[Continued on next page]

(54) Title: ELECTRONIC VOTING SCHEME EMPLOYING PERMANENT BALLOT STORAGE



WO 01/022200 A2

(57) Abstract: Disclosed is a system for recording records, such as electronic ballots in an electronic scheme. A web server posts a web page having a ballot box. Individual voters receive and submit to the web page electronic ballots reflecting their votes. The web server computer permanently stores each received electronic ballots using a Write-Once, Read-Many (WORM) drive or similar device to prevent ballots from later being erased or altered. Election results may then be tallied, and the results of such tallying, together with the received ballots, transmitted or provided to a third-party authority to review the election results.



Published:

- *without international search report and to be republished upon receipt of that report*

(48) Date of publication of this corrected version:

8 August 2002

(15) Information about Correction:

see PCT Gazette No. 32/2002 of 8 August 2002, Section II

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

**ELECTRONIC VOTING SCHEME EMPLOYING
PERMANENT BALLOT STORAGE**

TECHNICAL FIELD

The following relates generally to electronic voting schemes.

BACKGROUND

The Internet is increasingly being used to conduct a variety of activities, including research, communication or document exchange, and "electronic commerce," in part, because it facilitates electronic communications with large databases, between individuals, and between vendors and purchasers. The Internet comprises a vast number of computers and computer networks interconnected through communication channels. One individual can use a personal computer to connect via the Internet to another's computer. In the field of electronic commerce, although many commercial transactions performed today could be performed electronically, the acceptance and widespread use of electronic commerce depends, in large part, upon the ease-of-use of conducting such electronic commerce or other activities. For example, if electronic commerce can be easily conducted, then even the novice computer user will choose to engage in such activities. Therefore, it is important that techniques be developed to facilitate conducting such activities electronically.

The Internet facilitates conducting activities electronically, in part, because it uses standardized techniques for exchanging information. Many standards have been established for exchanging information over the Internet, such as electronic mail, Gopher, and the World Wide Web ("WWW"). The WWW service allows a server computer system (*i.e.*, web server or web site) to send graphical web pages of information to a remote client computer system. The remote client computer system can then display the web pages.

Each resource (e.g., computer or web page) of the WWW is uniquely identifiable by a Uniform Resource Locator ("URL"). To view a specific web page, a client computer system specifies the URL for that web page in a request (e.g., a HyperText Transfer Protocol ("HTTP") request). The request is forwarded to the web server that supports that web page. When that web server receives the request, it sends the requested web page to the client computer system. When the client computer system receives that web page, it typically displays the web page using a browser. A browser is typically a special-purpose application program for requesting and displaying web pages.

Currently, web pages are often defined using HyperText Markup Language ("HTML") although other standards are on the horizon. HTML provides a standard set of tags that defines how a web page is to be displayed. When a user makes a request to the browser to display a web page, the browser sends the request to the server computer system to transfer to the client computer system an HTML document that defines the web page. When the requested HTML document is received by the client computer system, the browser displays the web page as defined by the HTML document. The HTML document contains various tags that control the display of text, graphics, controls, and other features. The HTML document may contain URLs of other web pages available on that server computer system or on other server computer systems.

The World Wide Web portion of the Internet is especially conducive to conducting electronic commerce, and a host of other activities that individuals have previously performed manually or over the phone. One activity that has been difficult to transfer to the Internet or Word Wide Web has been voting. An electronic voting scheme must ensure the privacy of each voter, as well as provide strict audit trails so that election officials or independent observers can verify no fraud has occurred. Furthermore, as with many electronic commerce techniques, such an electronic voting scheme must be easy for voters to use. Ballot types must range from simple yes/no

initiatives to complex multi-way candidate races allowing for the possibility of write-in candidates. The ballots must be tamper free, and must be sufficiently non-transitory, so that months after an election, the ballots and results can be reviewed by some independent authority. To date, the inventors are unaware of any system that fulfills these requirements.

BRIEF DESCRIPTIONS OF DRAWINGS

The headings provided herein are for convenience only, and do not affect the scope or meaning of the claimed invention.

Figure 1 is a block diagram illustrating an environment for use with an embodiment of the invention.

Figure 2 is a block diagram illustrating one embodiment for permanently storing electronic ballots for use with the environment of Figure 1.

Figure 3 is a flow diagram showing steps performed by the embodiment of Figure 2.

Figure 4 is a block diagram illustrating an alternative embodiment for permanently storing electronic ballots for use with the environment of Figure 1.

DETAILED DESCRIPTION

Aspects of the invention overcome limitations of the prior art and provide numerous additional benefits. In one embodiment of the invention, ballots are permanently stored using a Write-Once, Read-Many (WORM) drive. This prevents anyone, such as election officials, hackers, etc., from erasing votes or altering ballots from an electronic "ballot box". The electronic ballot box is formed as one or more web pages in an electronic "bulletin board" or voting website hosted by one or more web servers. Alternative embodiments employ other permanent data storage devices, as explained below.

The following description provides specific details for a thorough understanding of, and enabling description for, embodiments of the invention.

However, one skilled in the art will understand that the invention may be practiced without these details. In other instances, well known structures and functions have not been shown or described in detail to avoid unnecessarily obscuring the description of the embodiments of the invention.

Some of the detailed description provided herein is explicitly disclosed in the provisional patent applications; much of the additional material will be recognized by those skilled in the relevant art as being inherent in the detailed description provided in the provisional patent applications, or well known to those skilled in the relevant art. Those skilled in the relevant art can readily implement aspects of the invention based on the detailed description provided in the provisional patent applications.

Figure 1 and the following discussion provide a brief, general description of a suitable computing environment in which aspects of the invention can be implemented. Although not required, embodiments of the invention will be described in the general context of computer-executable instructions, such as routines executed by a general-purpose computer, such as a personal computer or web server. Those skilled in the relevant art will appreciate that aspects of the invention (such as for small elections) can be practiced with other computer system configurations, including Internet appliances, hand-held devices, multiprocessor systems, microprocessor-based or programmable consumer electronics, network PCs, mini computers, cell phones, mainframe computers, and the like. Aspects of the invention can be embodied in a special purpose computer or data processor that is specifically programmed, configured or constructed to perform one or more of the computer-executable instructions explained herein. The invention can also be practiced in distributed computing environments where tasks or modules are performed by remote processing devices, which are linked through a communications network, such as a Local Area Network (LAN), Wide Area Network (WAN), and the Internet. In a distributed computing environment,

program modules or sub-routines may be located in both local and remote memory storage devices.

Unless described otherwise, the construction and operation of the various blocks shown in Figure 1 and 2 are of conventional design. As a result, such blocks need not be described in further detail herein, as they will be readily understood by those skilled in the relevant art.

Referring to Figure 1, a suitable environment of system 100 includes one or more voter or client computers 102, each of which includes a browser program module 104 that permits the computer to access and exchange data with the Internet, including web sites within the World Wide Web portion 106 of the Internet. The voter computers 102 may include one or more central processing units or other logic processing circuitry, memory, input devices (e.g., keyboards and pointing devices), output devices (e.g., display devices and printers), and storage devices (e.g., fixed, floppy, and optical disk drives), all well known but not shown in Figure 1. The voter computers 102 may also include other program modules, such as an operating system, one or more application programs (e.g., word processing or spread sheet applications), and the like. As shown in Figure 1, there are N number of voter computers 102, representing voters 1, 2, 3 . . . N .

A server computer system 108, coupled to the Internet or World Wide Web ("Web") 106, performs much or all of the ballot collection, storing and other processes. A database 110, coupled to the server computer 108, stores much of the web pages and data (including ballots) exchanged between the voter computers 102, one or more voting poll computers 112 and the server computer 108. The server computer system 108, including the database 110, may employ security measures to inhibit malicious attacks on the system and to preserve the integrity of the ballots and other data stored therein.

The voting poll computer 112 is a personal computer, server computer, mini-computer, or the like, positioned at a public voting location to permit members of the public, or voters who may not have ready access to

computers coupled to the Internet 106, to electronically vote under the system described herein. Thus, the voter computers 102 may be positioned at individual voter's homes, where one or more voting poll computers 112 are located publicly or otherwise accessible to voters in a public election. The voting poll computer 112 may include a local area network (LAN) having one server computer and several client computers or voter terminals coupled thereto via the LAN to thereby permit several voters to vote simultaneously or in parallel.

Under an alternative embodiment, the system 100 may be used. In the context of a private election, such as the election of corporate officers or board members. Under this embodiment, the voter computers 102 may be laptops or desktop computers of shareholders, and the voting poll computer 112 can be one or more computers positioned within the company (e.g., in the lobby) of the company performing the election. Thus, shareholders may visit the company to access the voting poll computer 112 to cast their votes. One or more optional authority or organization computers 114 may also be coupled to the server computer system 108 via the Internet 106. The authority computers 114, in certain electronic voting schemes, each hold a key necessary to decrypt the tally of electronic ballots stored in the database 110. Threshold cryptographic systems require that a subset t of the total number of authorities n (i.e., $t < n$) agree to decrypt the ballots, to thereby avoid the requirement that all authorities are needed for ballot decryption. The authority computers 114 may provide decryption shares based on their keys to the server computer system 108 after the voting period ends so that the server computer system may decrypt the tally results.

The server computer 108 includes a server engine 120, a web page management component 122, a database management component 124, as well as other components shown more clearly in Figure 2. The server engine 120 performs, in addition to standard functionality, performs one or more electronic voting protocols, such as the protocols described in U.S. Patent

Application No. _____, filed March 24, 2000, entitled "Multi-way Election Method and Apparatus," and assigned to the same assignee as this invention. Thus, the server engine 120 performs all necessary ballot transmission to authorized voters, ballot collection, verifying ballots (e.g., checking digital signatures and passing verification of included proofs of validity in ballots), vote aggregation, ballot decryption and/or vote tabulation.

The web page component 122 handles creation and display or routing of web pages such as an electronic ballot box web page, as described below. Voters and users may access the server computer 108 by means of a URL associated therewith, such as <http://www.votewhere.net>, or a URL associated with the election, such as a URL for a municipality. The municipality may host or operate the server computer system 108 directly, or automatically forward such received electronic ballots to a third party vote authorizer who may operate the server computer system. The URL, or any link or address noted herein, can be any resource locator.

The web page management process 122 and server computer 108 may have secure sections or pages that may only be accessed by authorized people, such as authorized voters or system administrators. The server computer 108 may employ a secure socket layer ("SSL") and tokens or cookies to authenticate such users. Indeed, for small elections, or those where the probability of fraud is low (or results of fraud are relatively inconsequential), the system 100 may employ such simple network security measures for gathering and storing votes as explained below, rather than employing complex electronic encrypted ballots, as described in the above-noted patent application. Methods of authenticating users (such as through the use of passwords), establishing secure transmission connections, and providing secure servers and web pages are known to those skilled in the relevant art.

Referring to Figure 2, a more detailed representation of the server computer system 108 is shown. The server computer system 108 includes a router 202 coupled between the Internet 106 and a firewall 204. The router 202

acts as an interface between the Internet 106 and the server computer system 108. The router 202 receives incoming electronic ballots or votes produced by the voter computers 102 or voting poll computer 112, and routes them through the firewall 204 to a web-load balancing system 206.

The firewall 204 protects the server computer system 108 from attacks or security breaches directed at the system from the Internet 106. Any of various known firewall systems may be employed, such as those employing screened subnet architecture (e.g., packet filtering), and multi-homed host architecture (e.g., application gateway or dedicated proxy methods), although any of the many known firewall architectures may be employed.

The web-load balancing system 206 balances load on several web server computers 208 (three of which are shown in Figure 2). Load balancing is a technique well known in the art for distributing the processing load between two or more computers, to thereby more efficiently process instructions and route data. In the present context, the web-load balancing system 206 helps distribute received electronic ballots evenly between the web servers 208, which can be particularly important at peak traffic times.

As shown in Figure 2, each of the web servers 208 include internally or have coupled thereto write-once, read-many (WORM) drives 210. As explained more fully below, the WORM drives 210 permanently store received electronic ballots. Thus, in addition to the database 110 which stores the ballots for rapid access and processing by the web servers 208, the WORM drives 210 permanently store such ballots in the event of a catastrophic fault, or to later verify election results, as noted below. As shown by the broken lines in Figure 2, the web load balancing device 206 may directly route received ballots to the WORM drives 210 (as opposed to having such ballots first being directed to the web servers 208).

The web-load balancing system 206 acts as an interface to the WORM drives 210 to provide load balancing for such drives so that all electronic ballots are permanently stored on the WORM drives in an efficient

manner, particularly during times of peak traffic, and to overcome relatively slow write times (as compared to, for example, random access memory (RAM) write times). Each of the web servers 208 executes a software enabled application programming interface (API) running as a service thereon to enable writing of the electronic ballots onto the associated WORM drive 210. APIs for interfacing an application program such as the ballot collection and vote tallying process noted above and the writing of received ballots to the WORM drives 210 is similar to conventional APIs for permitting application programs for writing data to WORM drives or other similar drives. Several web servers 208 and WORM drives 210 are employed for not only efficient load balancing of received web traffic and/or electronic ballots, but also for redundancy and fault tolerance reasons. Indeed, while only a single router 202, firewall 204 and web-load balancing system 206 are shown in Figure 2, the server computer system 108 may employ two or more such devices/systems to further improve fault tolerance for the system. To further improve processing efficiency, the web servers 208 may employ cryptographic accelerator cards or math coprocessors not shown to expedite cryptographic functions when the server computer system 108 execute cryptographically complex electronic elections. Likewise, the voting poll computer 112 and/or voter computers 102 can employ such cryptographic accelerator cards or math coprocessors for similar reasons.

Any of several known WORM drives may be employed, such as Model No. CMO R540 MO, by Sony Corporation, Model No. HP5200ex SureStore, by Hewlett Packard, and Model No. T6-5200, by Maxoptix. These drives typically employ a 5.2 inch (13.2 centimeter) diameter, optical disk or cartridge, enhanced polycarbonate-type continuous composite WORM (CCW), having up to 5.2 Gigabytes of storage. Once data, such as electronic ballots, has been written to the optical disks in the WORM drives 210, the data may not later be erased or altered. In other words, such WORM drives 210 permit data to be permanently stored thereon once, and then thereafter read therefrom numerous times.

Other permanent data storage devices are possible. Digital Versatile Disk (DVD) drives may be used instead of the WORM drives 210. DVD drives offer wide support on various computing platforms, as well as high capacity, wide feature set, numerous drivers supporting such disks, low cost, and the like. CD-Write once media may also be employed, but may suffer from low memory capacity when used with large elections employing encrypted ballots.

Other permanent data storage media and associated data storage devices may be used, and may be desirable in certain elections. For example, the web servers 208 may be coupled to one, or a bank of, smart cards, printed circuit boards or cartridges containing programmable read-only memory (PROM), electronically programmable read-only memory (EPROM), and the like. Such memory may provide faster write times than WORM drives, but may be less tamper resistant and more expensive, particularly for elections with numerous voters and large ballots. Other computer-readable media may include magnetic disk drives, Bernoulli cartridges, and flash memory cards, if sufficient safeguards are employed (both hardware and software) to ensure that ballots stored thereon are tamper proof and not subject to fraud once ballots had been written thereto.

Under one embodiment, the server computer system 108 provides a website or "bulletin board" to which each voter posts his or her digitally signed electronic ballot. The server computer system 108 permanently stores each ballot in the database 110, so that ballots may not be altered or erased, as described herein. Once the predetermined polling period ends ("the polls close"), the web server computer system 108 verifies each ballot and aggregates or tallies them to produce a final tally, although verification, and some or all portions of ballot aggregation, decryption and tallying can be performed as ballots are received (or "on the fly").

Referring to Figure 3, a process 300 performed by the server computer system 108 and voting organization providing such system is shown.

To illustrate the processes 300 for gathering and storing electronic ballots, each component or step is generally described as a single function performed by the server computer system 108 (or authority employing such system). One skilled in the relevant art will appreciate that each of these components or steps may be implemented as several separate routines or subroutines.

In step 302, the server computer system 108 provides electronic ballots to authorized voters. Voters may be authorized in any number of processes, such as those described in U.S. Patent Application No. _____, filed March 24, 2000, entitled "Method, Article and Apparatus for Registering Registrants, Such As Voter Registrants" and assigned to the assignee of the present invention. Each electronic ballot includes all predetermined voting issues, instructions for voting, and any relevant cryptographic keys or processes.

Additionally, each electronic ballot includes a digital signature provided by the server computer system 108. Thus, voters who receive such ballots may check the digital signature to ensure that the ballot has not been corrupted or altered.

Under step 302, the electronic ballots may be emailed to each of the authorized voters. Under this method, the database 110 includes the email addresses, URLs, links or other logical addresses for the voter computers 102 and voting poll computer 112. The server computer system 108 then automatically retrieves each logical address and forwards the appropriate electronic ballot to each address. Alternatively, the server computer system 108 may provide a web page to be accessed by the voting computers 102 and voting poll computer 112. By accessing such web page, and proving authentication of the relevant voter, the voter may then download from the server computer system 108 an electronic ballot. These two methods of electronic ballot distribution represent server initiated and client initiated distribution methods; of course, many other similar methods may be employed whereby the server computer system 108 forwards electronic ballots to

authorized users, or where the voter computers 102 and voting poll computer 112 request electronic ballots.

In step 304, the server computer 108 receives electronically signed ballots from the voters. In one embodiment, the server computer system 108 provides the above-noted web page bulletin board that allows each voter to post his or her ballot thereto during a predetermined voting period. Of course, other methods for receiving electronic ballots are possible, including email, wireless data transmission (e.g., via cell phone or portable/wearable computer), and the like. The server computer 108 may provide a digitally signed receipt to the voter recognizing receipt of the voter's electronic ballot. Furthermore, the server computer 108 may first provide such receipt to one or more of the authority computers 114 who in turn add their digital signatures before forwarding the receipt to the voter.

After the predetermined voting period ends, the server computer 108 no longer permits additional ballots to be received and written to the WORM drive 210. Under an alternative embodiment, the server computer system 108 continues to collect additional ballots after the predetermined voting period, but flags each ballot as being late or otherwise provides some indication about when such ballots were received. The web server computer 208, under this alternative embodiment, does record such late ballots via the WORM drives 210.

In step 306, the web servers 208 in the server computer system 108 write each received ballot to the WORM drives 210 or other permanent data storage media devices. In general, it is desirable to write each ballot received under step 304 immediately to one of the WORM drives 210 under step 306. Under an alternative embodiment, the server computer system 108 may employ solid state memory (e.g., RAM) or other electronic memory buffers to buffer and hold electronic ballots temporarily before being written to one of the WORM drives 210. Such electronic buffers are particularly useful during peak traffic times, however, may suffer from possible security

shortcomings in that a fraudulent voting organization could tamper with electronic ballots, when in the buffer, before they are written to the WORM drives 210.

In step 308, the server computer system 108 verifies each received ballot. The verification can include checking the digital signature of each received ballot, and verifying the validity of each ballot, such as verifying correct hash function output and/or proofs of validity, such as under zero knowledge proofs. Such verification can be performed as the server computer system 108 sequentially reads each ballot previously written to the WORM drives 210. Alternatively, the server computer system 108 can perform some or all of such verification of received ballots before step 306 (before they are written to the WORM drives 210). For example, the server computer system 108 can verify the digital signature or compute the hash function of each ballot before writing it to the WORM drives 210. If the digital signatures do not verify or the computer hash function results do not match, the server computer system 108 may discard such ballots, and not write them to the WORM drives 210. However, third party voting verification authorities may request that all received ballots be permanently stored before any unauthorized ballots are discarded.

In step 310, the server computer system 108 aggregates the stored ballots and decrypts the results, with a threshold number of authorities if such an encryption protocol is employed. Ballot authorization and decryption under a threshold number of authorities is described in greater detail in the Multi-Way Election Method and Apparatus application noted above.

In step 312, the voting organization providing the server computer system 108 may provide the storage data to a voter verification authority. For example, the voting organization may provide one or more WORM disks from the WORM drives 210 to a third party organization who verifies that no fraud had occurred during the vote or ballot tabulation. Any method of physically

transferring the WORM disks to such a third-party vote verifying organization may be employed, including courier services.

Under an alternative embodiment, the server computer system 108 may employ a one-way hash function or simple error correction/detection technique (e.g., cyclic redundancy check (CRC)) to the data, or groups of data stored on the WORM disk. The server computer system 108, at predetermined times, or after a predetermined number of electronic ballots have been received, perform such a hash function or other method to provide an additional level of security and verification to ballots stored by the WORM drives 210. The results of the hash function are then likewise stored by the WORM drive, and can be presented to and verified by the third-party voting verification authority.

In step 314, the voting organization running the server computer system 108 and/or third-party voting verification authority may destroy the WORM disks after a predetermined time period. Many elections require that all ballots be saved or stored for a predetermined time period during which third parties may challenge or review election results to ensure that no fraud occurred. After such predetermined time period, however, the ballots typically must be destroyed. Therefore, the WORM disks may then be destroyed in step 314, to thereby effectively eliminate all electronic ballots. Of course, the voter computers 102 may each have stored thereon, their own ballots, but this option is left to each voter.

Under one embodiment of the invention, which employs the protocols described in the above-noted patent application, electronic ballots may be digitally signed by each authorized voter and posted by the voters to an area on a bulletin board or website representing a "ballot box." Ballots are encrypted by the voters but never decrypted. Multi-way elections are possible using both discrete log, elliptic curve and general group cryptosystems, all of which employ homomorphic properties to allow ballots to be combined to produce encrypted tallies. This multi-way election scheme ensures universal verifiability since any third party can see who voted without

seeing how they voted and duplicate the combination of the encrypted ballots to obtain the encrypted tally. Ballots are accompanied with zero-knowledge proofs of validity to ensure that a voted ballot includes only allowable options, without leaking any information about which ballot option the voter chose. Such proofs are non-interactive and all received ballots are automatically stored permanently by the WORM drives 210. The encrypted tallies are decrypted by t of n authorities without reconstructing the authorities' private key, using threshold encryption techniques. The decryption protocol requires a zero-knowledge proof which ensures that the correct ciphertext (ballot) has been decrypted using the private-key share corresponding to the authorities' group public-key. Further, compromise of the voter privacy would require a conspiracy of at least t of the n number of authorities.

The server computer system 108, with the WORM drives 210 or other permanent data storage devices, are useful for not only storing electronic ballots, but also for registering preregistered write-in candidates for elections, and other data for write-in candidates and votes. Under the multi-way election method and apparatus application noted above, a write-in candidate submits his or her name, ballot or precinct identifier and a race identifier. The server computer system 108 generates a candidate number for the identified race and computes a unique encryption generator. The candidate's name, ballot identifier, race identifier, candidate number and generator are stored by the WORM drive 210. Before the beginning of the election, registration of new write-in candidates is closed, and information for all write-in candidates is read from the WORM drive 210 by the server computer 108 and added to the appropriate electronic ballots before such ballots are distributed to voters. All received ballots are then stored on the WORM drive 210, together with any and all votes for preregistered write-in candidates.

Under an alternative method for write-in candidates described in the above application, a database is created containing a record for each person eligible to hold any office appearing on the ballot. The record contains the

person's name, unique identifier and an encryption generator. For any given race, the voter may fill in the name of a write-in candidate on the electronic ballot. The server computer system 108 then queries the database for that name, and if a match is found, the unique identifier and any necessary encryption data are used to form the vote for that candidate on the electronic ballot. The WORM drive 210 may be used to create a permanent record of such database for all eligible people to hold office on a given ballot. This permanent record could then be later reviewed by a third-party vote verification authority to ensure that all relevant names were included in the database.

Referring to Figure 4, an alternative embodiment of the invention is depicted as a system 400. As shown in Figure 4, the web server computers 208 are coupled directly to the internet 106, such as by means of only SSL and TCP/IP ports. Thus, the web servers 208 have only a limited command set and are thus more secure than platforms coupled to the internet by means of a router or other high functionality/command set devices.

The web servers 208 are coupled to an array of WORM drives 210 by means of a distributed file server 402. A distributed file server or system is a type of file system in which the file system itself manages and transparently locates pieces of information (e.g. ballots) from remote files and distributes files across a network, such as the LAN effectively formed by the web servers, WORM drives and distributed file server shown in Figure 4. The distributed file server 402 also manages read and write functions to the WORM drives 210 and database 110. The distributed file server 402 may be a process running on each, or one of, the web servers 208, or on a separate hardware device. Indeed, one of the web servers 208, WORM drives 210, and the database 110 may be enclosed within a single box to form a "vote engine" that may be connected directly to the Internet 106 as a stand alone product.

The distributed file server 402 receives ballots from the web servers 402 and determines which of several WORM drives 210 to instruct to write the ballot. The distributed file server 402 also stores the received ballots

in the database 110 for rapid access and rapid write-time with respect to the web servers 208. When one of the web servers 208 wishes to retrieve one of the ballots or some other file, the request is provided to the distributed file server 402, which in turn identifies where the ballot or desired file is stored, retrieves such ballot/file, and provides it to the web server.

As shown in Figure 4, one of the authority computers 114 also includes a WORM drive 210 coupled thereto. Under the embodiment described above where the authority computers receive and digitally sign ballot receipts for the voter computer 102 (recognizing that the voter's electronic ballot has been received), the authority computer may store such receipts. To enhance data integrity, such received receipts may be stored in the WORM drive 210. Thus, the authority computer can ensure that the web server computers 208 have not eliminated any ballots from the final tally. Of course, the authority computer 114 may receive and store on the WORM drive 210 other information, including ballots that may be forwarded thereto, and the like.

One skilled in the art will appreciate that the concepts of the invention can be used in various environments other than the Internet. For example, the concepts can be used in an electronic mail environment in which electronic mail ballots or forms are processed and stored. In general, a web page or display description (e.g., the bulletin board) may be in HTML format, email format, or any other format suitable for displaying information (including character/code based formats, bitmapped formats and vector based formats). Also, various communication channels, such as local area networks, wide area networks, or point-to-point dial-up connections, may be used instead of the Internet. The various transactions may also be conducted within a single computer environment, rather than in a client/server environment. Each voter or client computer may comprise any combination of hardware or software that interacts with the server computer or system. These client systems may include television-based systems, Internet appliances and various other consumer products through which transactions can be performed.

In general, as used herein, a "link" refers to any resource locator identifying a resource on the network, such as a display description of a voting authority having a site or node on the network. In general, while hardware platforms, such as voter computers, terminals and servers, are described herein, aspects of the invention are equally applicable to nodes on the network having corresponding resource locators to identify such nodes.

Unless the context clearly requires otherwise, throughout the description and the claims, the words 'comprise', 'comprising', and the like are to be construed in an inclusive sense as opposed to an exclusive or exhaustive sense; that is to say, in the sense of "including, but not limited to". Words using the singular or plural number also include the plural or singular number, respectively. Additionally, the words "herein", "hereunder", and words of similar import, when used in this application, shall refer to this application as a whole and not to any particular portions of this application.

The above description of illustrated embodiments of the invention is not intended to be exhaustive or to limit the invention to the precise form disclosed. While specific embodiments of, and examples for, the invention are described herein for illustrative purposes, various equivalent modifications are possible within the scope of the invention, as those skilled in the relevant art will recognize. The teachings of the invention provided herein can be applied to other record storage systems, not necessarily the electronic voting system described above.

The various embodiments described above can be combined to provide further embodiments. All of the above references and U.S. patents and applications are incorporated by reference. Aspects of the invention can be modified, if necessary, to employ the systems, functions and concepts of the various patents and applications described above to provide yet further embodiments of the invention.

These and other changes can be made to the invention in light of the above detailed description. In general, in the following claims, the terms

used should not be construed to limit the invention to the specific embodiments disclosed in the specification and the claims, but should be construed to include all ballot or record storage systems that operate under the claims to provide a method for permanently storing such data. Accordingly, the invention is not limited by the disclosure, but instead the scope of the invention is to be determined entirely by the claims.

CLAIMS

1 1. An electronic voting system for use with a computerized
2 network, comprising:

3 a plurality of voting computers coupled to the computerized
4 network, wherein each voting computer provides an electronic encrypted ballot
5 representing at least one vote;

6 a server computer system coupled to the computerized network,
7 wherein the server computer system includes:

8 at least one server computer for receiving the plurality of
9 electronic ballots from the plurality of voting computers, performing at
10 least one cryptographic operation relative to the plurality of electronic
11 ballots, and determining a tally of the votes; and

12 a write-once, read-many data storage device coupled to the
13 server computer and having a computer-readable medium therein,
14 wherein the server computer and data storage device are configured to
15 permanently write the plurality of received electronic ballots to the
16 computer-readable medium.

1 2. The system of claim 1, further comprising:

2 at least one voting poll computer coupled to the computerized
3 network and providing another plurality of electronic encrypted ballots to the
4 server computer system;

5 at least one authority computer coupled to the computerized
6 network that provides at least one cryptographic key for decrypting at least a
7 portion of the plurality of electronic ballots and the another plurality of
8 electronic ballots; and

9 wherein the server computer system includes at least one router
10 coupled to the computerized network, and at least one firewall coupled between
11 the router and the server computer.

1 3. The system of claim 1, further comprising:
2 at least one voting poll computer coupled to the computerized
3 network, wherein the voting poll computer is coupled to a plurality of
4 additional terminals over a network to receive, and provide to the server
5 computer system, another plurality of electronic encrypted ballots.

1 4. The system of claim 1 wherein the computerized network
2 includes the World Wide Web, wherein each of the plurality of voting
3 computers include a web browser program, and wherein the server computer
4 system includes:

5 at least two web server computers, each having at least one of the
6 data storage devices, wherein at least one of the web server computers provides
7 a ballot box web page for the plurality of voting computers to post their
8 respective electronic ballots thereto, and

9 a load balancing and fault tolerance system coupled between the
10 World Wide Web and the two web server computers, wherein the load
11 balancing and fault tolerance system is configured to provide substantially
12 equal numbers of the plurality of electronic ballots to the two web servers and
13 data storage devices, and to detect for and reroute received electronic ballots if
14 one of the two web server computers suffers a fault.

1 5. The system of claim 1 wherein the computer-readable
2 medium in the data storage device is a removable optical disk.

1 6. The system of claim 1 wherein the plurality of voter
2 computers include at least one palm-sized computer, cell phone, wearable
3 computer, interactive television terminal or Internet appliance.

1 7. A computer system for receiving a plurality of electronic
2 ballots over a network, comprising:

3 at least one server computer for receiving the plurality of
4 electronic ballots from the network, and performing at least one
5 operation relative to the plurality of electronic ballots; and

6 a permanent data storage device coupled to the server
7 computer and having a computer-readable medium, wherein the server
8 computer and data storage device are configured to write the plurality of
9 received electronic ballots to the computer-readable medium in an
10 unalterable fashion, and wherein the electronic ballots may be read from
11 the computer-readable medium thereafter.

1 8. The system of claim 7 wherein the electronic ballots are
2 encrypted and represent votes from a plurality of voters, wherein at least one
3 authority computer coupled to the network provides at least one cryptographic
4 key to the server computer for decrypting at least a tally from the plurality of
5 electronic ballots, and wherein the system further comprises:

6 at least one router coupled to the computerized network, and
7 at least one firewall coupled between the router and the server
8 computer.

1 9. The system of claim 7 wherein the network includes the
2 World Wide Web, and wherein the server computer system includes:

3 at least two web server computers coupled to the World Wide
4 Web;

5 at least two data storage devices coupled respectively to the two
6 web server computers, wherein at least one of the web server computers
7 provides a ballot box web page for receiving the electronic ballots.

1 10. The system of claim 7 wherein the server computer system
2 includes:

3 at least two server computers, each having one of the data storage
4 devices, and

5 a load balancing system coupled between the network and the
6 two server computers, wherein the load balancing system is configured to
7 distribute the plurality of electronic ballots to the two servers, the data storage
8 devices, or both.

1 11. The system of claim 7 wherein the data storage device is a
2 write-once, read-many (WORM) drive.

1 12. The system of claim 7 wherein the data storage device is a
2 CD-R drive.

1 13. The system of claim 7 wherein the data storage device is a
2 digital versatile disk (DVD) drive.

1 14. The system of claim 7 wherein the data storage device is a
2 removable structure, and wherein the computer-readable medium includes,
3 secured to the structure, programmable read only memory (PROM) or
4 electronically programmable read only memory (EPROM).

1 15. The system of claim 7 wherein the server computer
2 receives at least some of the plurality of electronic ballots from at least one
3 palm-sized computer, cell phone, wearable computer, interactive television
4 terminal or Internet appliance.

1 16. The system of claim 7 wherein the server computer
2 performs a hash or error detection operation on at least one set of the electronic
3 ballots stored by the data storage device, and wherein the data storage device
4 stores a result of the operation on the computer-readable medium.

1 17. The system of claim 7 wherein the server computer
2 performs an authentication or verification operation on at least one set of the
3 received electronic ballots and does not cause the data storage device to store
4 those electronic ballots that fail the authentication or verification operation.

1 18. The system of claim 7 wherein the server computer adds a
2 late flag to at least one set of the plurality of electronic ballots stored by the
3 data storage device, wherein the late flag indicates that the set of electronic
4 ballots were received outside of a predetermined time period.

1 19. The system of claim 7 wherein the server computer is
2 configured to receive write-in candidate data and wherein the server computer
3 and data storage device are configured to write the write-in candidate date to
4 the computer-readable medium in an unalterable fashion.

1 20. The system of claim 7, further comprising: another
2 permanent data storage device having a computer-readable medium for storing
3 at least some of the plurality of received electronic ballots thereto; and

4 a distributed file server communicating with the permanent data
5 storage device and the another permanent data storage device, and which
6 receives the electronic ballots and determines to which of the data storage
7 devices to route the received electronic ballots.

1 21. In an electronic voting system having a data processing
2 device coupled to a network for receiving a plurality of electronic ballots, an
3 apparatus comprising:

4 a permanent data storage device coupled to the data processing
5 device and having a computer-readable data storage medium, wherein the data
6 storage device is configured to receive the plurality of received electronic
7 ballots from the data processing device and to write the plurality of received
8 electronic ballots to the computer-readable medium in an unalterable fashion,
9 and wherein the data processing device may read the electronic ballots from the
10 computer-readable medium thereafter, but not alter or delete any of the
11 electronic ballots.

1 22. The apparatus of claim 21 wherein the electronic ballots
2 are encrypted and represent votes from a plurality of voters, wherein the
3 network includes the World Wide Web having a virtual ballot box for receiving
4 the plurality of electronic ballots, wherein the computer-readable data storage
5 medium is an optical disk and wherein the optical disk forms a permanent
6 record for electronic ballots posted to the virtual ballot box.

1 23. The apparatus of claim 21 wherein the electronic ballots
2 are encrypted and wherein the permanent data storage device stores the
3 encrypted electronic ballots.

1 24. The apparatus of claim 21 wherein the data storage device
2 is a write-once, read-many (WORM) drive.

1 25. The apparatus of claim 21 wherein the data storage device
2 is a CD-R drive.

1 26. The apparatus of claim 21 wherein the data storage device
2 is a digital versatile disk (DVD) drive.

1 27. The apparatus of claim 21 wherein the data storage device
2 is a removable structure, and wherein the computer-readable medium includes,
3 secured to the structure, programmable read only memory (PROM) or
4 electronically programmable read only memory (EPROM).

1 28. The apparatus of claim 21 wherein the data processing
2 device performs a hash or error detection operation on at least one set of the
3 plurality of electronic ballots stored by the data storage device, and wherein the
4 data storage device stores a result of the operation on the computer-readable
5 data storage medium.

1 29. The apparatus of claim 21 wherein the data processing
2 device adds a late flag to at least one set of the plurality of electronic ballots
3 stored by the data storage device, wherein the late flag indicates that the set of
4 electronic ballots were received outside of a predetermined time period.

1 30. A computer-readable medium for storing a computer
2 readable data structure, comprising:

3 a write-once, read-many computer readable medium having
4 written thereto a plurality of encrypted electronic ballots from a plurality of
5 voters, wherein each encrypted electronic ballot represents at least one vote
6 from one of the plurality of voters, wherein a data processing device may read
7 the plurality of encrypted electronic ballots from the write-once, read-many
8 computer-readable medium, but not alter or delete any of the encrypted
9 electronic ballots.

1 31. The apparatus of claim 30 wherein the data processing
2 device is an authority computer, and wherein the permanent data storage device
3 stores digitally signed receipts indicating receipt of received electronic ballots.

1 32. The computer-readable medium of claim 30 wherein the
2 write-once, read-many computer readable medium is a write-once, read-many
3 (WORM) optical disk.

4 33. The apparatus of claim 30, further comprising a distributed
file system communicating with the permanent data storage device, which
5 receives the electronic ballots from the data processing device.

7 34. The computer-readable medium of claim 30 wherein the
write-once, read-many computer readable medium is a CD-R disk.

9 35. The computer-readable medium of claim 30 wherein the
write-once, read-many computer readable medium is a digital versatile disk
10 (DVD) disk.

12 36. The computer-readable medium of claim 30 wherein the
write-once, read-many computer readable medium is a removable structure
13 having secured thereto programmable read only memory (PROM) or
14 electronically programmable read only memory (EPROM).

17 37. An electronic voting method, comprising:
18 receiving a plurality of electronic ballots from a plurality
of voters from a network;
19 performing at least one operation relative to the plurality
20 of electronic ballots; and

21 writing each of the plurality of received electronic ballots
22 to a computer-readable medium in an unalterable fashion.

4 distributing, over the network, a plurality of initial electronic
5 ballots to the plurality of voters;

6 receiving at least one cryptographic key from at least one
7 authority for decrypting at least a portion of the plurality of electronic ballots;

8 decrypting at least a tally of the electronic ballots based on the
9 received key or keys; and

10 providing the computer-readable medium to a third party verifier
11 after decrypting.

1 39. The method of claim 37 wherein receiving a plurality of
2 electronic ballots includes receiving the electronic ballots over the World Wide
3 Web, and wherein the method further comprises:

4 providing a ballot box web page for receiving the electronic
5 ballots.

1 41. The method of claim 37, further comprising:
2 performing a hash or error detection operation on at least one set
3 of the electronic ballots; and

4 storing a result of the operation on the computer-readable
5 medium.

1 42. The method of claim 37, further comprising performing an
2 authentication or verification operation on the plurality of received electronic
3 ballots.

1 43. The method of claim 37, further comprising:
2 adding a late flag to at least one set of the plurality of electronic
3 ballots, wherein the late flag indicates that the set of electronic ballots were
4 received outside of a predetermined time period; and
5 writing the set of electronic ballots to the computer-readable
6 medium with associated flags.

1 44. The method of claim 37 wherein the instructions are
2 performed in the order of receiving a plurality of electronic ballots, performing
3 at least one cryptographic operation, and writing each of the plurality of
4 received electronic ballots..

1 45. A computer-readable medium storing instructions for
2 instructing a computer coupled to a network, the instructions comprising:
3 receiving a plurality of electronic ballots from a plurality of
4 voters from the network; and
5 writing each of the plurality of received electronic ballots to a
6 computer-readable medium in an unalterable fashion.

1/4

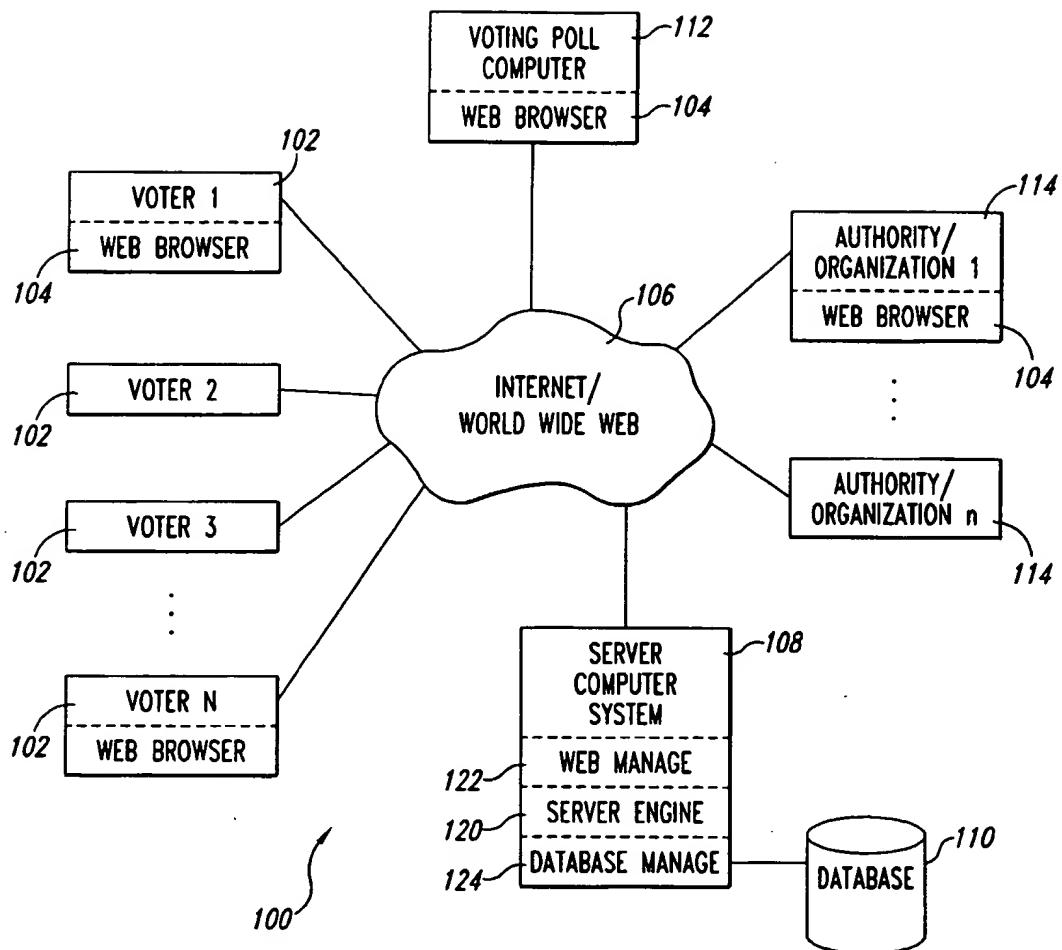
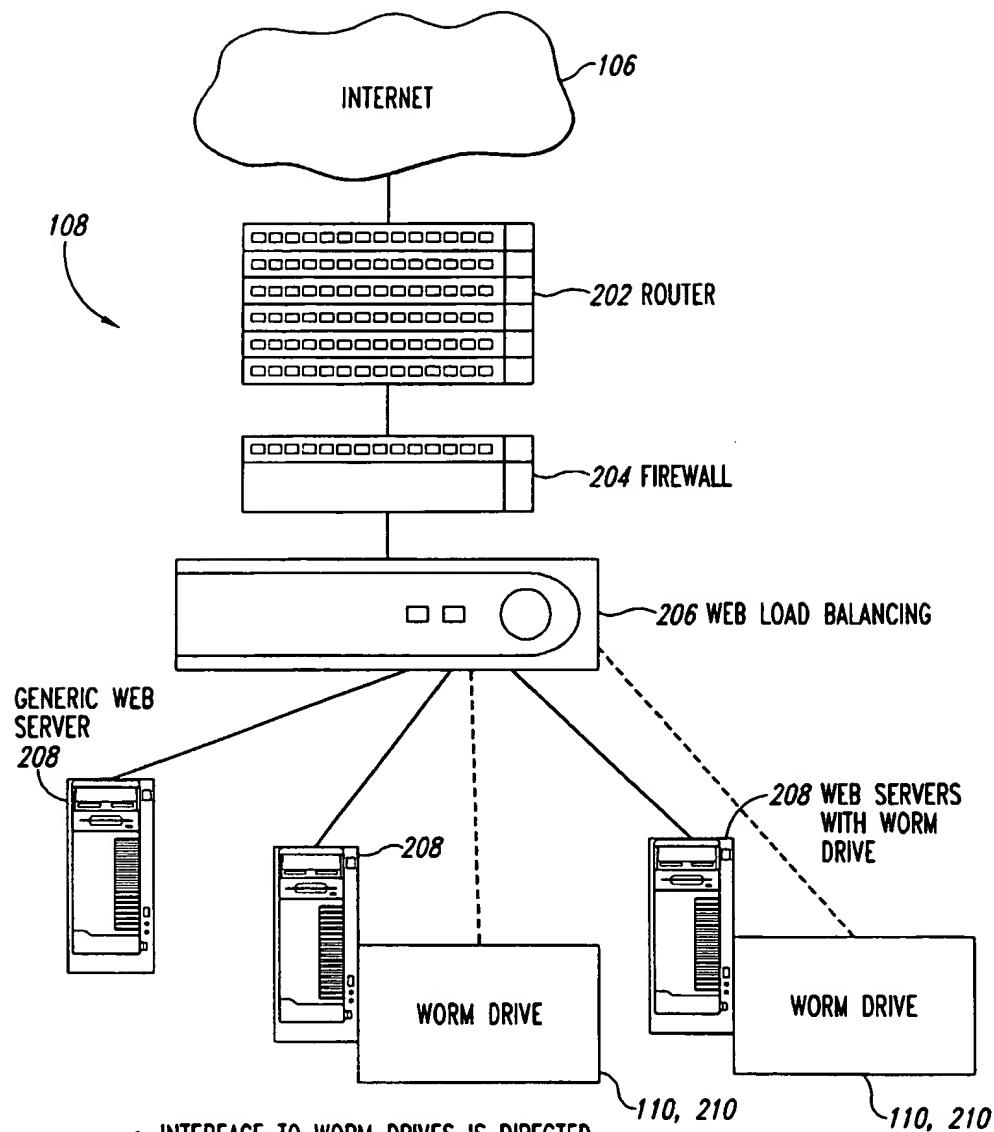


Fig. 1

SUBSTITUTE SHEET (RULE 26)

2/4



- INTERFACE TO WORM DRIVES IS DIRECTED THROUGH WEB LOAD BALANCING DEVICE TO PROVIDE LOAD BALANCING FOR WORM SERVICE.
- INTERFACE TO WORM DRIVES IS VIA A SOFTWARE API RUNNING AS A SERVICE ON THE WORM ENABLED WEB SERVERS.

Fig. 2

3/4

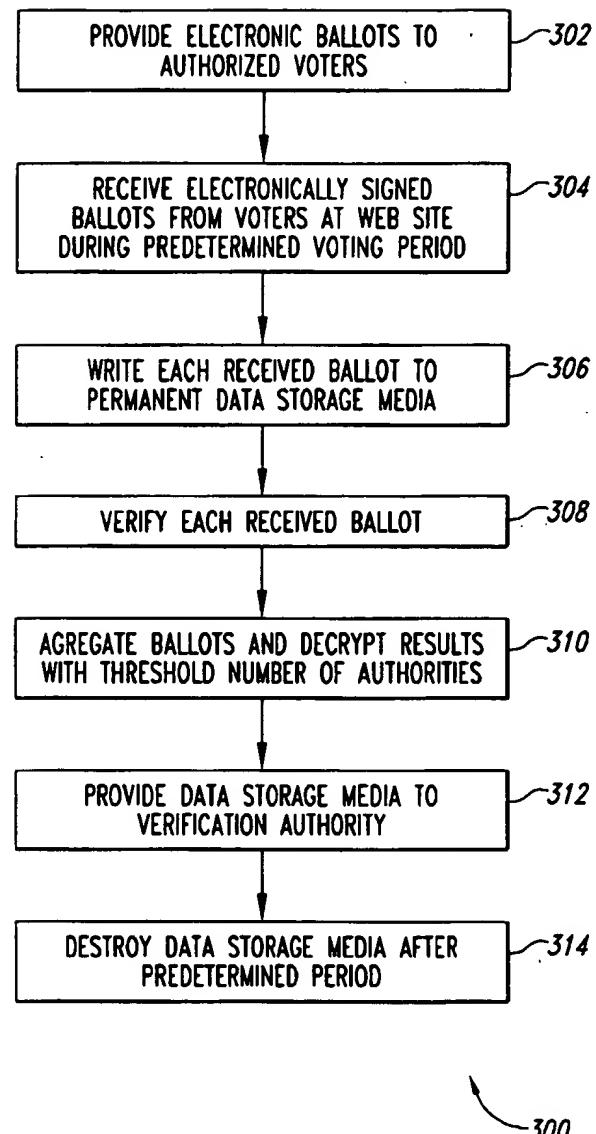


Fig. 3

4/4

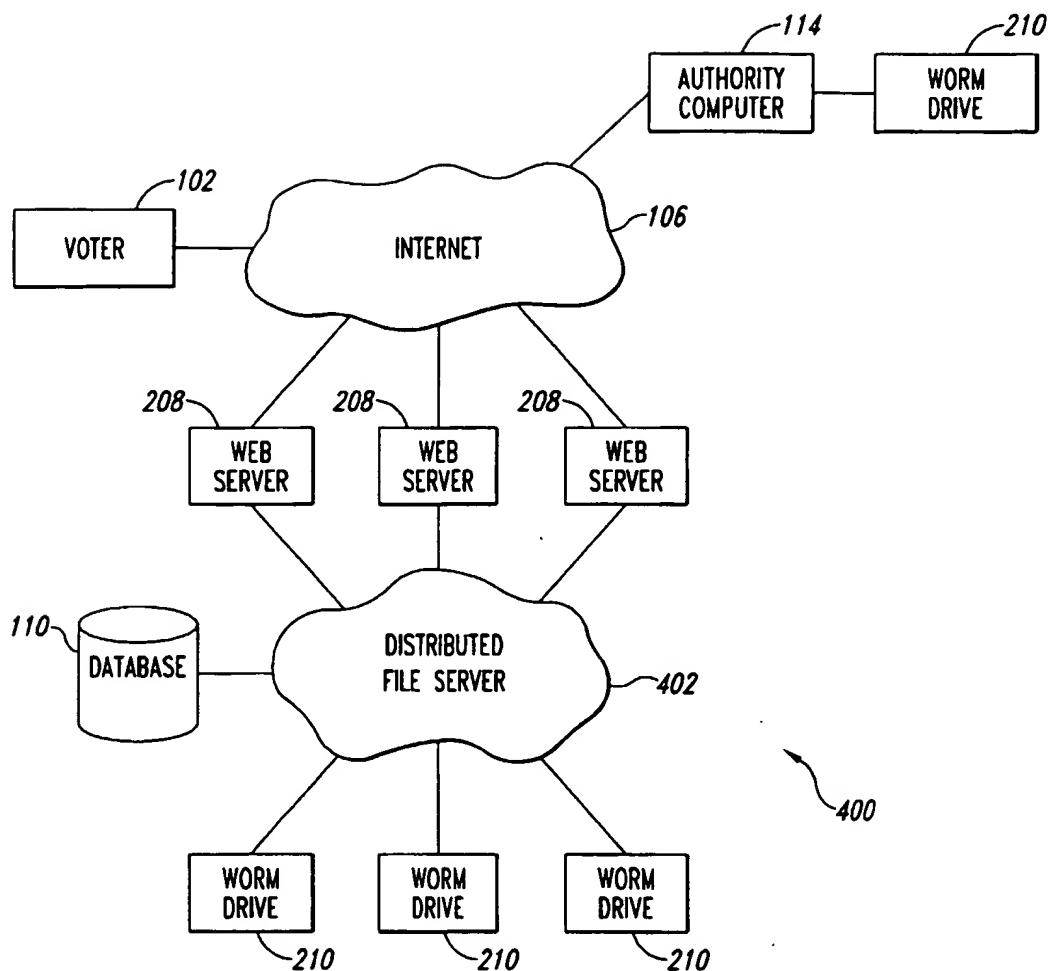


Fig. 4